The Design and Development of Hands-on Activities for Digital Forensics Education

Xinli Wang
School of Computing
Grand Valley State University
Allendale, Michigan, 49401 USA
wangx@gvsu.edu
0009-0007-0939-237X

Vijay Bhuse
School of Computing
Grand Valley State University
Allendale, Michigan, 49401 USA
bhusevij@gvsu.edu
0009-0009-6460-6048

Sara Sutton
School of Computing
Grand Valley State University
Allendale, Michigan, 49401 USA
suttosar@gvsu.edu
0000-0002-4669-8286

***Abstract*—It has been widely admitted by researchers and educators that hands-on activities are a core component in digital forensics education to help students gain practical skills that are needed in real-world forensic investigations. However, it is not clear in existing works about what kinds of hands-on activities are recommended to be integrated into a digital forensics course and how to design and develop them.**

In our teaching practice, hands-on activities for a digital forensics course are designed in three categories: 1) activities that assist students in learning how to use common digital forensics tools; 2) activities that help students gain in-depth understanding of the basic concepts and fundamental knowledge that are presented in class lectures; 3) activities that promote students the development of mindsets and data analytical skills that are needed for a digital forensic investigator. Various formats are employed to develop these hands-on exercises in different categories. The educational objectives and student learning outcomes map well to the CAE-CD (Centers of Academic Excellence - Cyber Defense) outcomes by completing their forensic knowledge units.

In this paper, we share our idea and experience to design and implement such hands-on assignments in each category for meeting specific educational objectives. Sample exercises are briefly described to explain our idea in each category. Open source tools and data sets are introduced for references. Experiences, lessons, and sample feedback from students are discussed. Our results will provide a point of reference for those who teach digital forensics courses at a college or university, or are developing a digital forensic curriculum.

Keywords—Digital Forensics; Education; Lab; Hands-on Activities

I. INTRODUCTION

Computer forensics (*a.k.a.* digital forensics) emerged as a branch of forensic science in early 1980s when the practitioners of law enforcement recognized the need to examine electronic data for identifying relevant digital evidence from a computer that was confiscated at a criminal scene [1]–[4]. With the growing use of the Internet and electronic devices, digital forensic investigations play an important role in most investigations of criminal and civil cases [5]–[7], the management of information technology (IT) systems to understand the 5-W and one H questions after an incident [8]–[12], and several other disciplines [6], [13]. As such, the U.S. Bureau of Labor Statistics has projected a strong growth in the need of digital forensics-related professionals [14], [15]. To meet this high demand for professionals with the expertise in the collection, examination, and analysis of electronic data, digital forensics has been offered as multidisciplinary courses in many colleges and universities world-wide [16]–[20] for both undergraduate and graduate students.

Similar with other branches of cybersecurity education, an important component for a digital forensics course is hands-on activities [20]–[22]. Lots of efforts have been invested by researchers, educators, and publishers to develop a variety of hands-on exercises. Examples include hands-on practices that come along with textbooks [23], [24], published lab manuals [25], [26], and commercial online labs [27], [28]. These existing materials have been used by many educators and helped them with developing and teaching courses on digital forensics. By following the step-by-step instructions described in the lab assignments, students will learn how to use common forensic tools for locating specified files (“catch the flag”). However, they cannot help students develop their analytic mindsets and problem-solving skills. One general comment from students is: “It is interesting to find the file. However, I am curious about why I want to do so.” As pointed out by earlier researchers [1], analytic mindsets and problem-solving skills are critical for a professional in digital forensic investigations.

Through an extensive review of existing literature in digital forensics education as outlined in Section II, we have discovered a lack of clear answers to the following questions:

1. What kinds of hands-on activities are needed for digital forensics education?
2. What are the educational objectives?
3. What are the specific learning outcomes associated with each lab?

With many years’ experience of teaching digital forensics at both undergraduate and graduate levels in a 4-year college, we have developed hands-on lab assignments in three different categories as briefly described in Table I. Although we update and develop new labs every year in the last several years, all updated and newly developed labs fall into these three categories. Students feedback has been positive and the learning outcomes are promising.

TABLE I. THREE CATEGORIES OF HANDS-ON ACTIVITIES

Tool Use: Students will learn how to use the tools that are used to complete the tasks for a digital forensic investigation through hands-on lab activities in this category.
Knowledge Reinforcement: Labs in this category are designed to reinforce the basic concepts and fundamental knowledge that are presented in class lectures.
Mindset Development: Lab assignments in this category are designed to help students develop the mindsets that are needed for an effective digital forensics investigator.

In this paper, we will explain the idea to design and develop such lab assignments for a digital forensics course, describe the educational objectives of the lab assignments in each category, elucidate how the learning outcomes of our lab assignments can be mapped to the outcomes through the completion of forensics knowledge units adopted by the CAE-CD (Centers of Academic Excellence - Cyber Defense) knowledge units [29], outline sample lab assignments that have been used in our classes, discuss our experiences and lessons, and share some student's feedback. Results of this work will be helpful to those who are teaching or going to teach a digital forensics course at a college or a university. Our experience can also be a point of reference for the curriculum development in digital forensics.

The rest of the paper is organized as follows. After introduction in this section, we will give a brief review of related works in the next section. Then we present the design and development of hands-on activities in each category in Section III. Sample assignments are also described briefly in this section to further expound our ideas and approaches for designing and to developing these lab assignments in each category. The educational objectives and learning outcomes of our proposed hands-on exercises are mapped well to the outcomes through the completion of CAE-CD forensics knowledge units in Section IV. We conclude our work and discuss our experiences and lessons in Section V. Finally, our thoughts for future work are briefly described in Section VI.

II. RELATED WORKS

Universities and colleges started to offer digital forensics courses in the early 1980s as a complement of computer security because the results of digital forensic investigations offered insights into why and how security system failed [19], [30]– [32]. As a new discipline in the education of forensic science and cybersecurity, earlier research works on digital forensics education were mainly focused on course development [33], [34], curriculum design and implementation [19], [31], [35]– [38], and textbook evaluation and selection [18]. With the fast increase in the demand for digital forensic professionals, degrees, programs, and concentrations in digital forensics have been offered at many colleges and universities around the world [39]–[43]. Liu [22], [44] gave a very comprehensive review on baccalaureate programs in computer forensics. Dafoulas *et al*. [45] presented a review of computer forensic programs in the United Kingdom, Europe, and the United States of America. Blauw and Leung [46] 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 topics according to how it is taught and who its audience are. A program of digital forensics might have various emphases 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 allocation, and so on [22], [44], [47], [48]. However, hands-on activities are an important component in all proposed and implemented curricula and programs. Early researches [30], [33] have outlined lab development and its challenges in digital forensics 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 electronic data. Some universities developed designated physical laboratories [31]. Some others implemented a virtual environment where forensic tools were installed and data containing intended digital evidence was loaded [49], [50]. Due to the sensitivity of digital forensic data and the nature of the destructive tendency of a forensic investigation, all data sets used in education were simulated data.

Some textbooks come with short descriptions of hands-on activities on specific topics [23], [24], [51]–[53]. Several sponsored projects have generated "realistic" forensic data sets to support digital forensics and cyber security education [54]–[56]. Most of them are so-called "catch the flag" (CF) activities. These exercises are helpful for the students to learn how to use common software tools for catching the intended artifacts.

More recently, Wang *et al*. [20] explained the idea to develop student's analytic mindsets with course projects. Gupta *et al*. [57] proposed a framework and format for developing digital forensics lab assignments. A set of shared instructional materials for digital forensics education is presented by Xu *et al*. [58]. Their recent works have been posted in a GitHub page and are publicly available [59]. Morris *et al*. provide an overview of what makes digital forensic examiners suffice from the viewpoints of different disciplines. The National Centers of Academic Excellence in Cybersecurity (NCAE-C) [29] has updated knowledge units of digital forensics and the corresponding outcomes. In the Centers of Academic Excellence - Cyber Defense (CAE-CD) document [29], the topics of digital forensics are classified into five disciplines (knowledge units): Device Forensics (DVF), Digital Forensics (DFS), Host Forensics (HOF), Media Forensics (MEF), and Network Forensics (NWF). Xu *et al*. have recently proposed the concept of Digital Forensic Artifact Generator (DFAG) and the DFAG-based knowledge units. They also define five principles to design digital forensics labs: real-world scenarios, comprehensive labs, problem-driven labs, self-paced learning, and an integrated open-source lab environment.

III. DESIGN AND DEVELOPMENT OF HANDS-ON ACTIVITIES

The main tasks of a digital forensic investigation are to collect, preserve, examine, and analyze electronic data, and finally present digital evidence related to a specific case. These can be effectively done only using appropriate tools along with relevant knowledge and the right mindsets and analytic skills. With our extensive experience of teaching digital forensics, we have designed and developed a set of hands-on assignments to help students achieve this goal. In this section, we will detail the design and development of these hands-on activities in the three categories that are briefly described in Table I. Example exercises will be given to further explain our ideas to design and develop them.

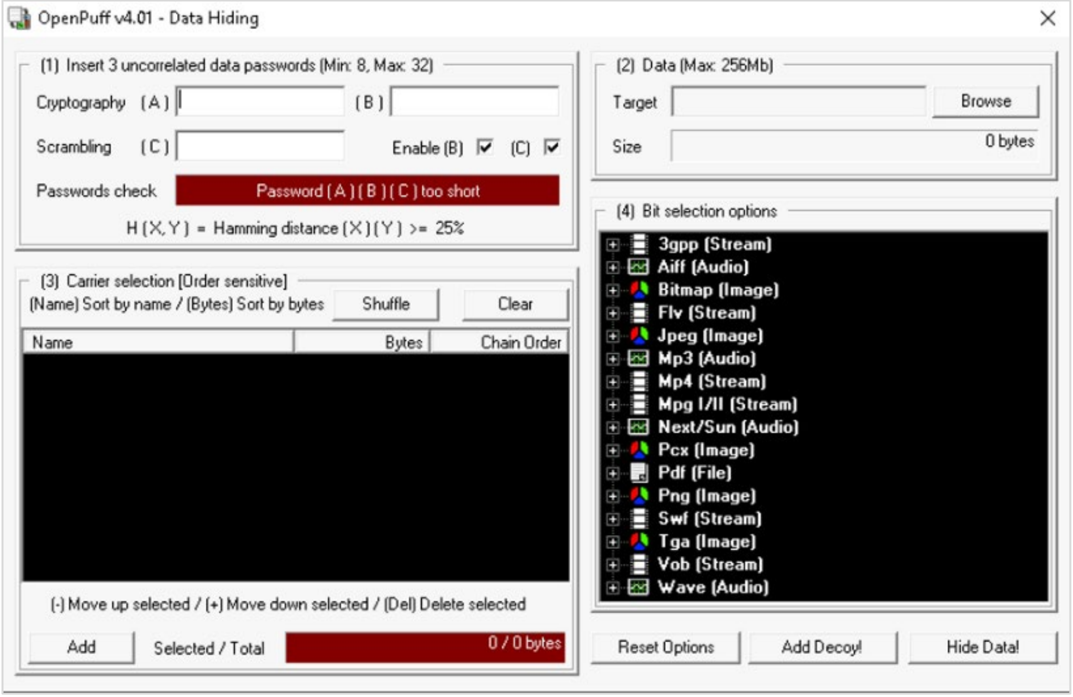
A. Labs for Tool Use

We have introduced a variety of software tools in the domain of free software that are widely used by digital forensic investigators and IT professionals. Examples include:

- **FTK® Imager:** FTK Imager [60] is introduced mainly to create a forensic friendly image of a physical disk or a logical disk (a partition), dump a snapshot of RAM memory, overview an existing forensic image to understand disk architectures, file systems, and file properties, export relevant files, and practice hash functions for data verification. It is also a good tool for beginners to recover deleted files from a physical disk and a partition.
- **Autopsy:** The Autopsy® Digital Forensics [61] is a widely used digital forensics tool in the domain of open source that provides the core features that are built in commercial forensic tools. It provides a graphical user interface to the Sleuth Kit® [62] and other digital forensics tools. We have used it in the labs of Windows forensics, Linux forensics, Photographic forensics, and Email forensics as a premier software tool for examining digital forensic images. Main functions include data carving, keyword search, timeline analysis, categorization of artifacts, Web artifacts, EXIF properties, bookmarking, report generation, file signature detection, and so on.
- **Volatility:** The Volatility Framework [63] is developed and well maintained by the Volatility Foundation. It is a widely used software package in the domain of open source for investigating memory dumps. We have used it in the labs of memory and malware forensics. In addition, we also introduced the Linux utility `strings` [64], which is included in a Kali Linux [65] installation. It is a very neat utility to convert binary files into human readable "strings". The results can be saved and searched for specific patterns.
- **Registry Viewer:** Access Data Registry Viewer [66] is commonly used for Windows registry forensics. We introduced it in one lab to examine Windows registry files.
- **OpenPuff:** The OpenPuff [67] software package is introduced as a steganography tool to investigate photographic files that may have hidden data. Although there are many other steganography tools for Windows [68] and for Linux [69], the OpenPuff stands out for educational purposes because of its support for a variety of file formats, including different formats of photographic image files, audio files, PDF files, and so on. You can also choose to use different percentages of bits in each pixel with bit selection options. Multiple files can be used to hide data in different formats (*e.g.*, plain text, graphics, or other files). Encryption is supported with the option of three different encryption keys. It is straightforward to learn to use it, even by a beginner, with its self-explainable instructions on the tabs and buttons. The screenshot shown in Fig. 1 exhibits a GUI for hiding data. As it is depicted, you can type in three different encryption keys in the left-top window. Multiple carrier files can be added to the left-lower dialogue box by clicking on the **Add** button. The percentages of the bits in each pixel you would like to use can be chosen under the ”Bit selection options” tab in the right-lower window.

In addition to the above standalone tools, we have also introduced commonly used Linux commands/utilities for the purpose of digital forensic investigation. Examples [70], [71] can be found from various posts on the Web.

The main educational objectives of the labs in this category are to help students learn how to use common forensic tools to examine a dataset and understand the functions the tools provide. We assume that students never used them when such labs were developed. In a lab for these purposes, we usually start with a high-level introduction to the tool. Then, a web link to the user manual (if available) is given. Good articles about the utilization of this tool are given if available. Then, we will give the download web page and ask students to download it directly from the Web and install it themselves on a virtual machine (VM) provided by the university. This exercise will help students understand where the tool can be obtained, the current version should be adopted, and learn how to use the tool themselves.



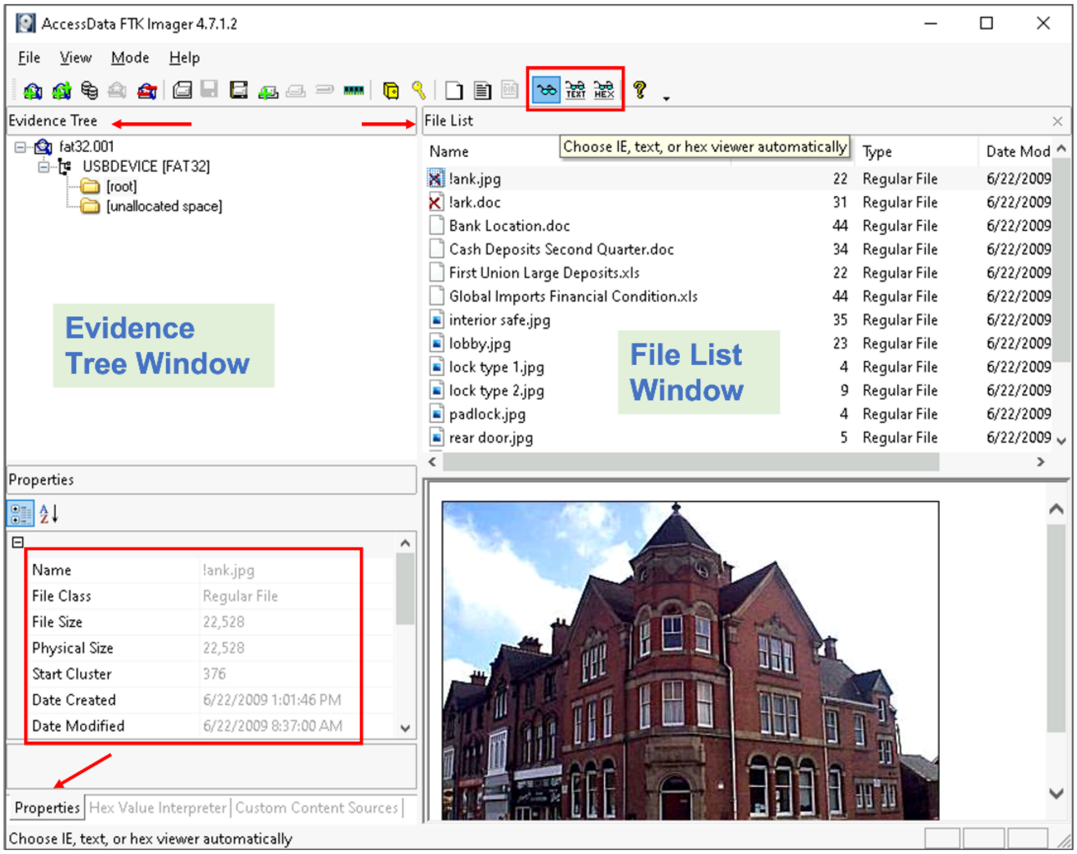
Password (A)(B)(C) too short

H(X,Y) = Hamming distance (X)(Y) >= 25%

Size: 0 bytes

Selected / Total: 0 / 0 bytes

Fig. 1. The GUI of OpenPuff for Data Hiding

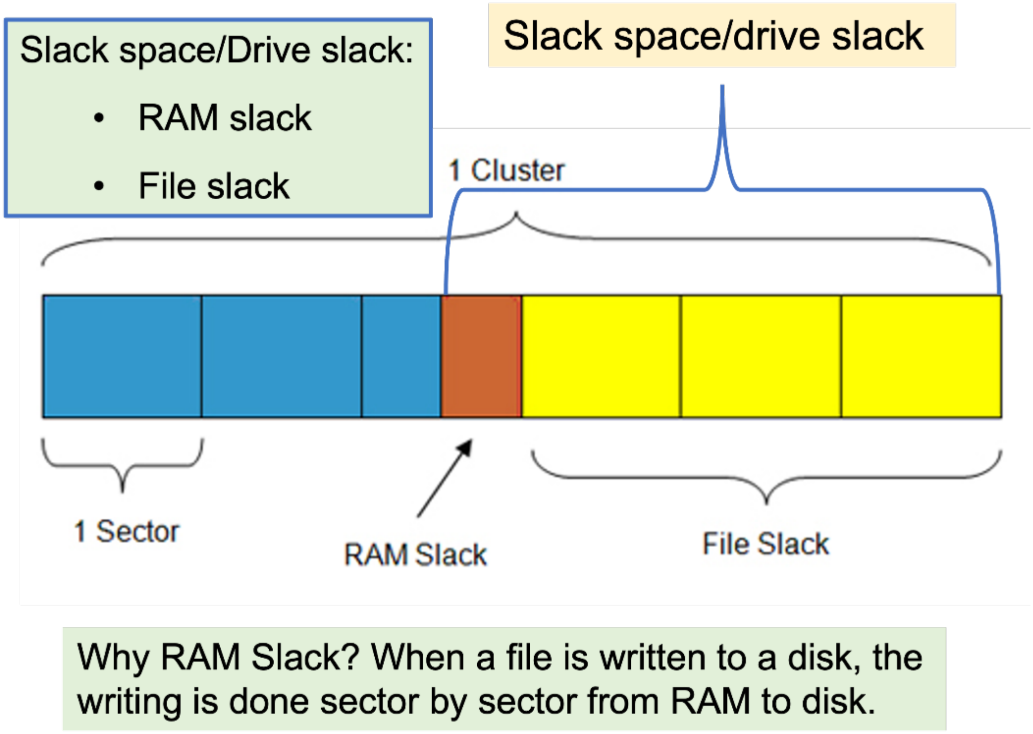


Name		Type	Date Mod
!ank.jpg	22	Regular File	6/22/2009
!ark.doc	31	Regular File	6/22/2009
Bank Location.doc	44	Regular File	6/22/2009
Cash Deposits Second Quarter.doc	34	Regular File	6/22/2009
First Union Large Deposits.xls	22	Regular File	6/22/2009
Global Imports Financial Condition.xls	44	Regular File	6/22/2009
interior safe.jpg	35	Regular File	6/22/2009
lobby.jpg	23	Regular File	6/22/2009
lock type 1.jpg	4	Regular File	6/22/2009
lock type 2.jpg	9	Regular File	6/22/2009
padlock.jpg	4	Regular File	6/22/2009
rear door.jpg	5	Regular File	6/22/2009

Name	!ank.jpg
File Class	Regular File
File Size	22,528
Physical Size	22,528
Start Cluster	376
Date Created	6/22/2009 1:01:46 PM
Date Modified	6/22/2009 8:37:00 AM

Choose IE, text, or hex viewer automatically

Fig. 2. A Demo of FTK Imager



Why RAM Slack? When a file is written to a disk, the writing is done sector by sector from RAM to disk.

Fig. 3. A Diagram of Slack Space/Drive Slack, RAM Slack, and File Slack

After software installation, detailed instructions are given with a dataset to help students get started with this tool. Screenshots with highlighted marks are used to show students what can be found and from where they can be seen. For example, the screenshot shown in Fig. 2 is given in a lab to help students learn how to use FTK Imager to view a file that is recovered from a given forensic image. The Evidence Tree window and File List window are highlighted. When a file is chosen, the contents of the file can be viewed in the bottom-right window with IE, a text viewer, and a hex viewer, respectively, by clicking on the corresponding button on the task bar. At the same time, the property values of this file can be viewed in the bottom-left window by clicking on the Properties tab.

B. Labs for Knowledge Reinforcement

The main educational objective of the labs in this category is to help students gain in-depth understanding of essential concepts and fundamental knowledge that are presented in class lectures. Labs are usually given after these materials have been covered in class. One way to develop such labs is to ask informative results after related information has been observed. For example, when students have observed the sizes of a sector and a cluster along with the physical and logical sizes of a file, a lab question can ask students to calculate the sizes in Bytes of drive slack, RAM slack, and file slack. After this exercise, students will gain a better understanding of these fundamental concepts about a disk architecture and learn the fact that disk space is allocated to a file cluster by cluster by the operating system and data is written to the disk sector by sector from the RAM memory.

$$\texttt{Drive Slack = RAM Slack + File Slack} \tag{1}$$

It is usually not easy for students to understand those concepts because they are not visible on a disk and the topic can be dry when it is presented in a lecture. From the student's feedback and the outcome of the course, such hands-on activities are a good way to help them comprehend these concepts and knowledge about the relationship between drive slack, RAM slack, and file slack, as expressed in Equation 1 and depicted in Fig. 3.

Another example in this category is to demonstrate the concepts of I-node, hard link, and soft link in a Linux system. We ask students to conduct a short experiment by creating a hard link and a soft link to an existing file. Then, we ask them to display the information of associated I-node, file size, and time stamps with the Linux command `ls -il`. Finally, we ask them to observe the results and summarize their discovery.

C. Labs for Mindset Development

With advanced technology and well-developed software tools, it is not very difficult to identify an artifact in a digital forensic investigation if an instigator knows what the artifact is and how to use the tools. However, the question is what are the artifacts I am looking for and how can I get started. This is especially true in the condition where an investigator faces a huge volume of data. Therefore, certain mindsets are needed for future digital forensic investigators to carry out their work. From the existing works [72]–[74] and our long-time teaching experience, the key mindsets include:

- **Analytic Thinking:** Digital forensic investigators need to think critically and analytically to examine electronic data, identify relevant evidence, and draw accurate conclusions. They must have a keen eye for details and the ability to connect various pieces of information to form a complete picture.
- **Technical Curiosity:** A digital forensic investigator should possess a natural curiosity and enthusiasm for new technology. They must keep up with the latest trends, tools, and techniques in the field of digital forensics. Being eager to learn and explore new technologies helps in staying ahead of the curve.
- **Objectivity:** Maintaining objectivity is crucial in digital forensics investigations. Investigators must approach their work without biases or preconceived notions. They should rely on facts, evidence, and scientific methodologies along with their knowledge to draw conclusions rather than personal beliefs or assumptions.
- **Patience and Persistence:** Digital forensics investigations can be time-consuming and require patience. Investigators often encounter complex challenges, encrypted data, or situations where data recovery is difficult. Having the persistence to overcome obstacles and the patience to meticulously analyze large amounts of data is vital.
- **Ethical Mindset:** Digital forensic investigators must adhere to a strict code of ethics. They deal with sensitive and confidential information. It is essential to maintain confidentiality, integrity, and professionalism throughout the investigation process. Upholding ethical standards is crucial for the credibility of the investigation and the legal proceedings that may follow.
- **Self-Learning:** Technology and techniques in the digital forensic field are constantly evolving. Investigators need to stay updated with the latest developments and methodologies by attending training sessions, conferences, and participating in professional forums. A commitment to lifelong learning ensures they remain effective in their role.
- **Collaboration and Teamwork:** Digital forensics investigations often involve working with various stakeholders, such as law enforcement, legal professionals, and IT teams. Each one has special expertise. Having strong interpersonal and communication skills is essential to collaborate effectively with others and work as part of a team. Sharing knowledge and expertise can lead to more successful outcomes.
- **Adaptability:** Future digital forensic investigators must be adaptable and flexible in their approach. Each investigation presents unique challenges, and they may need to adjust their methods and strategies accordingly. Being able to adapt to changing circumstances is crucial in this ever-changing field.

After the hands-on exercises in the first two categories, we design and develop hands-on activities in this category to help the future digital forensic analysts develop the mindsets they need to perform their work effectively. These activities are designed either as case studies or course projects. Both are implemented as teamwork. Case studies usually take one or two weeks, while a course project needs 4-6 weeks to complete. A lab of case study consists of a brief description about the case and the requirements to complete the investigation. An existing forensic image is provided, and hints may be given based on the difficult level of the case.

As an example, the following case study is derived from a course project in a previous class. The case has a short description as follows:

> *There is strong evidence to believe that Bob, CEO of Example Inc., colluded or conspired with Alice, the manager of Some Inc., in their business on illegal drugs and trades for high profits. A server belonging to the Example company has been seized with a warrant and an image has been created.*
>
> *We believe a central server has been used for communication between the two persons. 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.*

When the case was given as an assignment, the first question was where to start the investigation since the image contained several hundreds of files. With the hint of the time period when the events might occur, students usually start with a timeline analysis using Autopsy [61] to narrow down the target files, most of which were manipulated by their owner. For example, some of the file extensions were modified or changed on purpose. In addition, students found a steganographic tool that was widely used to hide data. As discussed in class, this type of clue itself might indicate that these files were suspicious. According to the recovered file signatures, 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 Fig. 4. At first glance, they were all ordinary photographs.

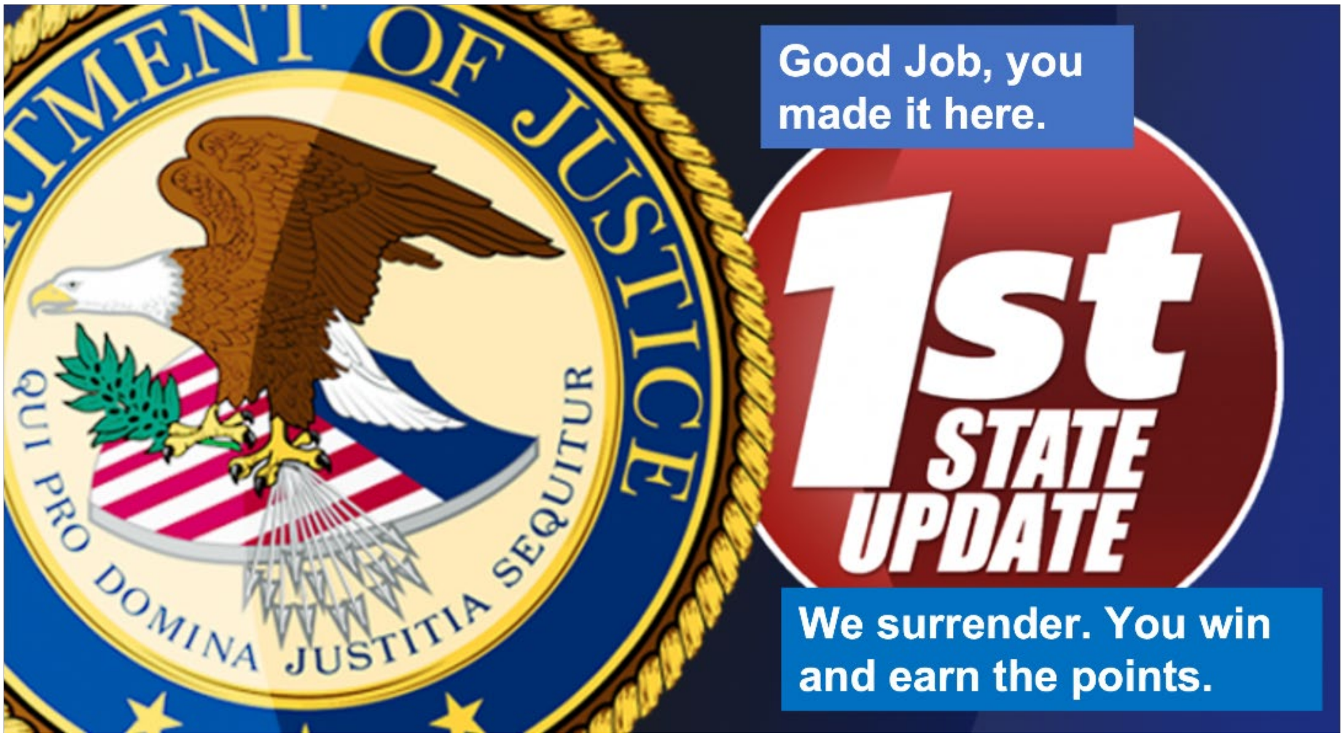

MENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
Good Job, you made it here.
1st STATE UPDATE
We surrender. You win and earn the points.

Fig. 4. An Example Image Recovered from the Case

Since those pictures looked like 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 that was identified in the given image. They were finally excited to discover critical evidence with the steganographic tool for this case. From there, they were able to successfully recover more relevant evidence.

IV. A MAP TO THE CAE-CD OUTCOMES

The knowledge units and outcomes by the completion of these knowledge units described in the document of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) [75], sponsored by the National Security Agency (NSA), are widely accepted as a good reference to design, develop, and deliver a curriculum in cybersecurity [58]. This section provides a map of the educational objectives and learning outcomes of the hands-on activities proposed in this paper to the CAE-CD outcomes by completing knowledge units in Device Forensics (DVF), Digital Forensics (DFS), Host Forensics (HOF), and Media Forensics (MEF) that have been recently updated in the CAE Cyber Defense Knowledge Units [29]. We do not cover much about network forensics (NWF) in hands-on activities due to the limits of time and equipment.

TABLE II. A MAP OF LEARNING OUTCOMES THROUGH THESE HANDS-ON ACTIVITIES TO THE CAE-CD OUTCOMES

Labs for tool use: “Use one or more common digital forensics tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.” “Students will be able to understand how to acquire a forensically sound image.”
Labs for knowledge reinforcement: “Describe what can/cannot be retrieved from various Operating Systems.” “Describe the methodologies used in host forensics.”
Labs for mindset development: “Students will be able to understand how to identify forensic artifacts left by attacks.” “Describe the steps in performing digital forensics from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, through the completion of legal proceedings.”

As shown in Table II, the design of our hands-on activities maps to the CAE-CD outcomes very well. We introduce several commonly used digital forensics tools in the category of tool use activities, including FTK Imager [60], Autopsy (SleuthKit) [61], and Volatility [63]. Through one of the labs, students have learned how to acquire a forensically friendly image of a logical disk and how to make a memory dump. Fundamental concepts and essential digital forensics knowledge are reinforced through the hands-on activities in the category of knowledge reinforcement. After completion of these hands-on exercises, students will be able to understand what can and cannot be recovered from various operating systems, including Windows, Linux, and MacOS. From the students' feedback we know that they have learned a lot through the hands-on activities in the category of mindset development. As described in the previous section, they have learned how to start a digital forensic investigation, how to examine the data to identify relevant artifacts, what the steps are for a digital forensic investigation through the development of analytic thinking, technical curiosity, and objectivity.

V. CONCLUSION AND DISCUSSION

We have proposed to design and develop hands-on activities in three categories for digital forensics education for meeting the needs of an effective digital forensics investigator, including tool use, knowledge reinforcement, and mindset development. The development of these exercises has been briefly described in each category. The educational objectives and learning outcomes of these hands-on activities map to the CAE-CD outcomes very well. Although some of the assignments are challenging, the course evaluation has been highly positive along with these labs. Students' feedback has been positive. We quote some of them here.

- "The course presented ideas in lectures then allowed us to work through a real-world example. I felt like I learned when I completed labs, and they made me think."
- "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."

Labs in the first category are designed to assist students in gaining hands-on experience with commonly used digital forensics tools, including FTK Imager [60], Autopsy (SleuthKit) [61], Access Date Registry Viewer [66], Volatility [63], and others. In this category, step-by-step instructions are given in a lab assignment. Like existing exercises [25]– [28], lab assignments can be developed with the techniques of "Catch the Flag" (CF) questions. As a new discipline, digital forensics has its own uniqueness [76] and fundamental knowledge units [29], [58]. Hands-on activities in the category of knowledge reinforcement are designed to help students gain in-depth understanding of the fundamental concepts and knowledge that have been discussed in class lectures. These concepts can be dry when presented in a class lecture. On the other hand, hands-on exercises create an active learning environment for students to understand them. As argued by Naqvi *et al*. [77], a good digital forensics investigator needs not only good understanding of related technologies but also excellent skills in problem solving and a strong mind-set in analysis. Hands-on activities in the category of mindset development are designed to promote the development of the mindsets needed by a digital forensic investigator that are summarized in Section III-C. Similar with existing works, these exercises are developed either as case studies [58], [59] or a course project [20]. To develop these assignments, we have downloaded data sets from Digital Corpora [78], [79], which have been used by early researchers [54]–[56], [80], and Volatility Foundation memory samples [81]. Although most of the data sets are old, they are fine for educational purposes.

In practice, we can certainly combine the hands-on activities in different categories in a single lab assignment, especially the activities in both categories of tool use and knowledge reinforcement. The key in the design and development of a lab is how to ask questions and why a question is asked. We do not want to ask a question for simply asking a question. Each question should be asked with a special educational objective that falls in one of the three categories listed in Table I.

VI. FUTURE WORK

Due to the limit of time and facilities, we have not covered network forensics and device forensics as defined in the CAE-CD knowledge units [29]. Materials developed by Xu *et al*. [59] can be a good resource for us to cover such topics in the future. The ideas and principles of zero-trust digital forensics [82] have been recently proposed and recognized to be helpful in various digital forensics investigations [83]– [85]. The main guideline for zero-trust digital forensics is to perform multifaceted verification before an artifact can be trusted because digital evidence can be easily modified, changed, and composed on purpose. We would like to design and develop hands-on activities to implement such guidelines in the future.

REFERENCES

[1] A. Yasinsac, R. F. Erbacher, D. G. Marks, M. M. Pollitt, and P. M. Sommer, "Computer forensics education," *IEEE Security & Privacy*, vol. 1, no. 4, pp. 15–23, July 2003.

[1] I. Charters, "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.

[2] R. Hankins, T. Uehara, and J. Liu, "A comparative study of forensic science and computer forensics," in 2009 *Third IEEE International Conference on Secure Software Integration and Reliability Improvement*. New York, NY, USA: IEEE, July 2009, pp. 230–239.

[3] M. Losavio, K. C. Seigfried-Spellar, and J. J. Sloan III, "Why digital forensics is not a profession and how it can become one," *Criminal Justice Studies*, vol. 29, no. 2, pp. 143–162, 2016.

[4] Science and Technology Select Committee, "Forensic science and the criminal justice system: a blueprint for change," *House of Lords, London*, vol. 3rd Report of Session 2017-19, pp. 1–66, 2019.

[5] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," *IEEE Access*, vol. 10, pp. 11 065–11 089, 2022.

[6] Australian Federal Police Media, "Sydney man charged with possessing and transmitting child abuse material," AFP Media: (02) 5126 9297, March 2022, https://www.afp.gov.au/news-media/media-releases/sydney-man-charged-possessing-and-transmitting-child-abuse-material. Last Accessed in May, 2023.

[7] C. Easttom, *System Forensics, Investigation, and Respons*e, 3rd ed. Burlington, MA, United States: Jones & Bartlett Learning, 2019.

[8] P. Kunert, "Insurance giant AON confirms it has suffered 'cyber incident'," The Register, March 2022, https://www.theregister.com/2022/03/01/aon_cyber_incident/. Last Accessed in May, 2023.

[9] E. Salfati and M. Pease, "Digital forensics and incident response (DFIR) framework for operational technology (OT)," NISTIR 8428, June 2022, https://doi.org/10.6028/NIST.IR.8428. Last Accessed in May, 2023.

[10] E. Barlow, "The what, when, where, who, how and why behind security incidents," SecurityHQ, on-line, October 2021, https://www.securityhq.com/blog/the-what-when-where-who-how-and-why-behind-security-incidents/. Last Accessed in May, 2023.

[11] M. B. Jimenez and D. Fernandez, "A framework for SDN forensic readiness and cybersecurity incident response," in 2022 *IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. New York, NY, USA: IEEE, 2022, pp. 112–116.

[12] S. Morris, M. Hadgkiss, A. David, J. Guinness, and C. Frewin, "We're making a list and we're checking it twice, gonna find out what makes digital forensic examiners suffice," *WIREs Forensic Science*, vol. e1487, pp. 1–12, 2023. [Online]. Available: https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/wfs2.1487

[13] Office of Occupational Statistics and Employment Projections, "Information security analysts," Occupational Outlook Handbook, U.S. Bureau of Labor Statistics, online, September 2022, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm. Last Accessed in May, 2023.

[14] ——, "Forensic science technicians," Occupational Outlook Handbook, U.S. Bureau of Labor Statistics, online, September 2022, https://www.bls.gov/ooh/life-physical-and-social-science/forensic-science-technicians.htm. Last Accessed in May, 2023.

[15] P. D. Dixon, "An overview of computer forensics," *IEEE Potentials*, vol. 24, no. 5, pp. 7–10, Dec 2005.

[16] S. E. Goodison, R. C. Davis, and B. A. Jackson, "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.

[17] J. Liu, L. Gottschalk, and K. Jian, "Textbooks for computer forensic courses: A preliminary study," in *Proceedings of Annual ADFSL Conference on Digital Forensics, Security and Law*. 4350 Candlewood Lane, Ponce Inlet, Florida 32127, USA: Association of Digital Forensics, Security and Law (ADFSL), 2007, pp. 141–146.

[18] S. Srinivasan, "Digital forensics curriculum in security education," *Journal of Information Technology Education: Innovations in Practice*, vol. 12, pp. 147–157, 2013.

[19] X. Wang, Y. Bai, and B. Goda, "Project design and implementation for digital forensics education," in *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, ser. SIGITE '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 33–38. [Online]. Available: https://doi.org/10.1145/3349266.3351402

[20] K. R. Lawrence and H. Chi, "Framework for the design of web-based learning for digital forensics labs," in *Proceedings of the 47th Annual Southeast Regional Conference*, ser. ACM-SE 47. New York, NY, USA: Association for Computing Machinery, 2009. [Online]. Available: https://doi.org/10.1145/1566445.1566546

[21] J. Liu, "Ten-year synthesis review: A baccalaureate program in computer forensics," in *Proceedings of the 17th Annual Conference on Information Technology Education*, ser. SIGITE '16. New York, NY, USA: ACM, 2016, pp. 121–126. [Online]. Available: https://dl.acm.org/doi/10.1145/2978192.2978226

[22] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 5th ed. Boston, MA, United States: Cengage Learning, 2016.

[23] ——, *Guide to Computer Forensics and Investigations*, 6th ed. Boston, MA, United States: Cengage Learning, 2019.

[24] ——, *Lab Manual for Nelson/Phillips/Steuart's Guide to Computer Forensics and Investigations*, 4th ed. Boston, MA, United States: Course Technology Press, 2010.

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

[26] INFOSEC Learning LLC, "We provide an online hands-on experience for skillset readiness in information technology," Online, 2020, https://www.infoseclearning.com/. Last Accessed in June, 2023.

[27] Cengage, "Cengage unlimited: Access to all your cengage course materials," Online, 2023, https://www.cengage.com/unlimited/. Last Accessed in June, 2023.

[28] National Centers of Academic Excellence in Cybersecurity (NCAE-C), "Welcome to the national centers of academic excellence in cybersecurity (NCAE-C)," Web page, online, June 2023, https://public.cyber.mil/ncae-c/. Last Accessed in June, 2023.

[29] G. A. Francia, III, "Digital forensics laboratory projects," *J. Comput. Sci. Coll.*, vol. 21, no. 5, pp. 38–44, May 2006. [Online]. Available: http://dl.acm.org/citation.cfm?id=1127351.1127360

[30] L. Batten and L. Pan, "Teaching digital forensics to undergraduate students," *IEEE Security Privacy*, vol. 6, no. 3, pp. 54–56, May 2008.

[31] W. A. Conklin, R. E. Cline, and T. Roosa, "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*, ser. HICSS '14. Washington, DC, USA: IEEE Computer Society, 2014, pp. 2006–2014. [Online]. Available: http://dx.doi.org/10.1109/HICSS.2014.254

[32] L. Troell, Y. Pan, and B. Stackpole, "Forensic course development," in *Proceedings of the 4th Conference on Information Technology Curriculum*, ser. CITC4 '03. New York, NY, USA: ACM, 2003, pp. 265–269. [Online]. Available: http://doi.acm.org/10.1145/947121.947180

[33] ——, "Forensic course development: One year later," in *Proceedings of the 5th Conference on Information Technology Education*, ser. CITC5 '04. New York, NY, USA: ACM, 2004, pp. 50–55. [Online]. Available: http://doi.acm.org/10.1145/1029533.1029547

[34] G. C. Kessler, "Online education in computer and digital forensics: A case study," in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. New York, NY, USA: IEEE, Jan 2007, pp. 264a–264a.

[35] N. A. Aziz, M. S. M. Yusof, M. H. B. A. Malik, A. Rasyad Hanizam, and L. H. Abd Rahman, "Acquiring and analyzing digital evidence - a teaching and learning experience in class," in *2018 Cyber Resilience Conference (CRC)*. New York, NY, USA: IEEE, Nov 2018, pp. 1–4.

[36] I. Palmer, E. Wood, S. Nagy, G. Garcia, M. Bashir, and R. Campbell, "Digital forensics education: A multidisciplinary curriculum model," in *Digital Forensics and Cyber Crime*, J. I. James and F. Breitinger, Eds. Cham: Springer International Publishing, 2015, pp. 3–15.

[37] S. Kiltz, J. Dittmann, and C. Vielhauer, "Supporting forensic design - a course profile to teach forensics," in 2015 *Ninth International Conference on IT Security Incident Management IT Forensics*. New York, NY, USA: IEEE, May 2015, pp. 85–95.

[38] L. Gottschalk, J. Liu, B. Dathan, S. Fitzgerald, and M. Stein, "Computer forensics programs in higher education: A preliminary study," *SIGCSE Bull.*, vol. 37, no. 1, pp. 147–151, Feb. 2005. [Online]. Available: http://doi.acm.org/10.1145/1047124.1047403

[39] G. C. Kessler and M. E. Schirling, “The design of an undergraduate degree program in computer & digital forensics,” *Journal of Digital Forensics, Security and Law*, vol. 1, no. 3, pp. 37–50, 2006.

[40] J. Liu, “Developing an innovative baccalaureate program in computer forensics,” in *Proceedings. Frontiers in Education. 36th Annual Conference*. 1005 Lausanne, Switzerland: Frontiers, Oct 2006, pp. 1–6.

[41] J. Liu, “Implementing a baccalaureate program in computer forensics,” *J. Comput. Sci. Coll*., vol. 25, no. 3, pp. 101–109, Jan. 2010. [Online]. Available: http://dl.acm.org/citation.cfm?id=1629116.1629134

[42] H. Chi, F. Dix-Richardson, and D. Evans, “Designing a computer forensics concentration for cross-disciplinary undergraduate students,” in *2010 Information Security Curriculum Development Conference*, ser. InfoSecCD ’10. New York, NY, USA: ACM, 2010, pp. 52–57. [Online]. Available: http://doi.acm.org/10.1145/1940941.1940956

[43] J. Liu, “Baccalaureate programs in computer forensics,” in *2016 IEEE International Conference on Electro Information Technology (EIT)*. New York, NY, USA: IEEE, May 2016, pp. 0615–0620.

[44] G. A. Dafoulas, D. Neilson, and S. Hara, “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)*. New York, NY, USA: IEEE, Oct 2017, pp. 144–154.

[45] F. F. Blauw and W. S. Leung, “ForenCity: a playground for self-motivated learning in computer forensics,” in *Information Security Education – Towards a Cybersecure Society*, L. Drevin and M. Theocharidou, Eds. Cham: Springer International Publishing, 2018, pp. 15–27.

[46] J. H. Riley, Jr., “Developing a baccalaureate digital forensics major,” in *Proceedings of ADFSL Conference on Digital Forensics, Security and Law*. 4350 Candlewood Lane, Ponce Inlet, Florida 32127, USA: Association of Digital Forensics, Security and Law (ADFSL), 2010, pp. 123–130.

[47] J. Liu, “An analysis of the students’ academic background in a computer forensics program,” *J. Comput. Sci. Coll*., vol. 28, no. 2, pp. 32–39, Dec. 2012. [Online]. Available: http://dl.acm.org/citation.cfm?id=2382887.2382894

[48] S. Garfinkel, “Lessons learned writing digital forensics tools and managing a 30tb digital evidence corpus,” *Digital Investigation*, vol. 9, pp. S80–S89, August 2012.

[49] E. K. Hawthorne and R. K. Shumba, “Teaching digital forensics and cyber investigations online: Our experiences,” *European Scientific Journal /SPECIAL/ edition*, vol. 2, pp. 1–7, September 2014, available online at https://eujournal.org/index.php/esj/article/view/4150. Last Accessed in June, 2019.

[50] B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, *Guide to Computer Forensics and Investigations*, 3rd ed. Boston, MA, United States: Course Technology Press, 2007.

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

[52] D. R. Hayes, *A Practical Guide to Computer Forensics Investigations*, 1st ed. Indianapolis, Indiana, USA: Pearson, 2015.

[53] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, “Bringing science to digital forensics with standardized forensic corpora,” Digit. Investig., vol. 6, pp. S2–S11, Sep. 2009. [Online]. Available: http://dx.doi.org/10.1016/j.diin.2009.06.016

[54] K. Woods, C. A. Lee, S. Garfinkel, D. Dittrich, A. Russell, and K. Kearton, “Creating realistic corpora for security and forensic education,” in *Proceedings of ADFSL Conference on Digital Forensics, Security and Law*. 4350 Candlewood Lane, Ponce Inlet, Florida 32127, USA: Association of Digital Forensics, Security and Law (ADFSL), 2011, pp. 123–134.

[55] Y. Yannikos, L. Graner, M. Steinebach, and C. Winter, “Data corpora for digital forensics education and research,” in *Advances in Digital Forensics* X, G. Peterson and S. Shenoi, Eds. Berlin, Heidelberg: Springer, 2014, pp. 309–325.

[56] K. Gupta, A. Neyaz, N. Shashidhar, and C. Varol, “Digital forensics lab design: A framework,” in 2022 *10th International Symposium on Digital Forensics and Security (ISDFS)*. New York, NY, USA: IEEE, 2022, pp. 1–6.

[57] W. Xu, L. Deng, and D. Xu, “Towards designing shared digital forensics instructional materials,” in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, vol. 1. New York, NY, USA: IEEE, 2022, pp. 117–122.

[58] F. Xu, “Free hands-on digital forensics labs for students and faculty,” GitHub Web Page, online, May 2023, https://github.com/frankwxu/digital-forensics-lab. Last Accessed in June, 2023.

[59] Exterro, “FTK® Imager,” Exterro® Web Page, June 2023, https://www.exterro.com/ftk-imager. Last Accessed in June, 2023.

[60] B. Carrier, “Autopsy Digital Forensics,” BasisTech® BasisTech LLC. Web page, June 2023, https://www.autopsy.com/. Last Accessed in June, 2023.

[61] ——, “The Sleuth Kit,” Home Page, June 2023, https://www.sleuthkit.org/sleuthkit/index.php. Last Accessed in June, 2023.

[62] The Volatility Foundation, “Volatility Foundation,” Web Page, 2020, https://www.volatilityfoundation.org/. Last Accessed in June, 2023.

[63] die.net, “Strings - print the strings of printable characters in files,” strings (1) - Linux man page, online, 2023, https://linux.die.net/man/1/strings. Last Accessed in June, 2023.

[64] OffSec Services Limited, “Kali – The most advanced Penetration Testing Distribution,” Kali Homepage, 2023, https://www.kali.org/. Last Accessed in June, 2023.

[65] Exterro, Inc., “Registry Viewer 2.0.0,” Exterro® Web Page, June 2023, https://www.exterro.com/ftk-product-downloads/registry-viewer-2-0-0. Last Accessed in June, 2023.

[66] Embedded SW, “OpenPuff - Yet not another steganography SW,” Embedded SW Homepage, 2023, https://embeddedsw.net/OpenPuff_Steganography_Home.html. Last Accessed in June, 2023.

[67] V. Kumar, “Top 10 free steganography tools for Windows 10 updated 2022,” CyberPratibha Blog, May 2022, https://www.cyberpratibha.com/blog/steganography-tools-for-windows-10/. Last Accessed in June, 2023.

[68] R. Red, “5 of the best steganography tools in Linux,” MakeTechEasier Web Page, March 2023, https://www.maketecheasier.com/best-steganography-tools-linux/. Last Accessed in June, 2023.

[69] Computer Hope, “Linux lsof command,” Web Page, August 2021, https://www.computerhope.com/unix/lsof.htm. Last Accessed in June, 2023.

[70] T. Fisher, “How to use the netstat command,” Web Page, April 2023, https://www.lifewire.com/netstat-command-2618098. Last Accessed in June, 2023.

[71] H. Jahankhani and A. Hosseinian-far, *Digital forensics education, training and awareness*, ser. Cyber Crime and Cyber Terrorism Investigator’s Handbook. United States: Elsevier Inc., jul 2014, pp. 91–100.

[72] S. Johnson, CI-DR™ *Key Capability Forensic Teams*. New York, NY, USA: IEEE, 2021, pp. 71–85.

[73] GoldFynch eDiscovery, “The digital forensics ’mindset shift’ attorneys can learn from,” Web post in Linkedin, March 2023, https://www.linkedin.com/pulse/digital-forensics-mindset-shift-attorneys-can-learn-from-goldfynch/#:~:text=Digital%20forensics%20involves%20gathering%20and%20analyzing%20digital%20data%20in%20a%20legally%20admissible%20way. Last Accessed in June, 2023.

[74] National Centers of Academic Excellence in Cybersecurity (NCAE-C), “2020 CAE Cyber Defense (CAE-CD) Knowledge Units,” CAE

Documents Library, online, June 2021, https://public.cyber.mil/ncae-c/documents-library/. Last Accessed in June, 2023.

[75] A. D. Irons, P. Stephens, and R. I. Ferguson, “Digital investigation as a distinct discipline: A pedagogic perspective,” *Digit. Investig*., vol. 6, no. 1-2, pp. 82–90, Sep. 2009. [Online]. Available: http://dx.doi.org/10.1016/j.diin.2009.05.002

[76] S. Naqvi, P. Sommer, and M. Josephs, “A research-led practice-driven digital forensic curriculum to train next generation of cyber firefighters,” in *2019 IEEE Global Engineering Education Conference (EDUCON)*. New York, NY, USA: IEEE, April 2019, pp. 1204–1211.

[77] Digital Corpora, “Home,” Web, online, May 2023, https://digitalcorpora.org/. Last Accessed in June, 2023.

[78] ——, “Corpora,” Web, online, May 2023, https://digitalcorpora.org/. Last Accessed in June, 2023.

[79] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digit. Investig*., vol. 7, pp. S64–S73, Aug. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.diin.2010.05.009

[80] Volatility Foundation, “Memory Samples,” GitHub, online, March 2019, https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples. Last Accessed in June, 2023.

[81] C. Neale, I. Kennedy, B. Price, Y. Yu, and B. Nuseibeh, “The case for zero trust digital forensics,” *Forensic Science International: Digital Investigation*, vol. 40, p. 301352, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266628172200021X

[82] C. Neale, “Fool me once: A systematic review of techniques to authenticate digital artefacts,” *Forensic Science International: Digital Investigation*, vol. 45, p. 301516, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281723000173

[83] P. Reedy, “Interpol review of digital evidence for 2019–2022,” *Forensic Science International: Synergy*, vol. 6, p. 100313, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2589871X22000985

[84] G. Gopan, A. Subramanian, B. S. K B, K. Duraipandian, and M. Sathiya-narayananan, “The intercorrelation between zero trust, dark web, and its implications in the field of digital forensics,” in *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*. New York, NY, USA: IEEE, 2023, pp. 197–203.