Generating Interest in Cybersecurity Through High School Digital Forensics Education

Patrick Pape
Mississippi State University
75 B.S. Hood Dr.
Mississippi State, Mississippi
pape@dasi.msstate.edu

John A. Hamilton Jr.
Mississippi State University
75 B.S. Hood Dr.
Mississippi State, Mississippi
hamilton@research.msstate.edu

ABSTRACT

This paper provides a look at the author's experiences and approach to teaching a varying range of students, from high school to those currently working in the field of digital forensics. With the increasing need for more cybersecurity professionals, it is important to expose students as soon as possible to the concepts of cybersecurity and the potential degree options that would allow the students to pursue jobs in the field. Though not limited to high school students, we will discuss the curriculum that we use when teaching high school students and other relative newcomers to the concepts of cybersecurity and digital forensics. Digital forensics is a relatively low-cost entry point to teaching new students about the field of cybersecurity and this makes it a great place for interested students to start. We combine freely available tools and operating systems with hands-on collaborative experience to reinforce discussions about various aspects of digital forensics and cybersecurity in general. Using our previous experiences with both high schoolers and professionals, this paper presents a curriculum for teaching high school students digital forensics in an outreach capacity.

Categories and Subject Descriptors

L.6 [**Computer Forensics**]: All; M.1.4 [**Professional Topics**]: Computing Education—*Computing education programs, k-12 education, adult education*

General Terms

Design, Human Factors, Security

Keywords

digital forensics, high school, education, cybersecurity, curriculum, outreach

1. INTRODUCTION

By exposing high school students to digital forensics and cybersecurity concepts in a time when they are making important choices about their future, we measure the capability to facilitate an interest in hard science and engineering degrees. This paper discusses previous successes dealing with high school students and digital forensics novices in a teaching capacity. The key to the work is the focus on a longitudinal study that tracks student feedback and the current state of the field and adjusts the course material and teaching strategy accordingly. We measure the impact of the courses on the students' interest in cybersecurity related fields and use that knowledge to reinforce the "best" parts of the course, as indicated by the students. What we present in this paper is our current course material, polished by years of experience and feedback with students, in a way that would facilitate easier access to high school students as an outreach program with the university.

The goal of these courses is to open up new pathways for high schools students to engage in cybersecurity related fields in their future careers. Much of our teaching material is posted online and we are in the progress of updating the material and establishing a more permanent location to disseminate material to interested students. By creating a freely accessible location for coursework and other learning aides, the students can further investigate digital forensics concepts and their interest in the subject. In addition to the high school students, an online repository is used as a place where anyone interesting in learning more about digital forensics can obtain lectures, guided exercises and customized virtual machine images to get started.

This work utilizes the feedback and experience of the digital forensics programs at two major southeastern universities to create courses that cater specifically to increasing the interest of high school students in science and engineering fields. Both authors have experience teaching digital forensics from the introductory to advanced levels. The feedback from the students from the teaching grants that funded these teaching experiences will help to shape the courses moving forward. By maintaining contact with the interested students, we can get the information we need about the influence our program has on a students decision to enter a cybersecurity field, as well as continuing to aid the students in seeking out and learning more about digital forensics and related subjects.

Digital forensics is a strong avenue for introducing students and novices to the fields of cybersecurity because the cost of entry is relatively low. Utilizing freely available tools and operating systems and combining that with our teaching program, the students are able to seek out the experience and knowledge they get from the workshops and online materials, without having to worry about affording registration in the program and what goes with it. This is especially important when dealing with the lower income and underrepresented populations in the states where we run these programs. Students who could otherwise grow to be exceptional applicants to cybersecurity programs may not have the chance to be exposed to digital forensics and cybersecurity concepts.

2. RELATED WORK

There has been an increasing amount of attention paid to establishing digital forensics educational programs at varying levels of education, including: high school, undergraduate, and professional. This recent work helps to serve as the foundation for our initial approach to designing classes and engaging with our students across the country. Work like [2] looks at how to build digital forensics labs to effectively facilitate cybersecurity and digital forensics degrees at the college level. Details about the equipment used to construct the lab and about the process for conducting digital forensics in the lab is discussed. Other proposed approaches to building effective digital forensics labs are discussed in [7] and [12], where emphasis is placed on maintaining a current level of digital forensics knowledge and efficiently disseminating the information to those who seek training from the labs. The lab designs discussed in these papers favor an active learning style that uses practical examples and open-ended hands-on examples for instruction.

An example of an outreach program established for digital forensics training is found in [17]. This paper describes the process of establishing a forensics training center to address the need for training for individuals capable of dealing with the increasing number of cyber crimes. A program for instructing military personnel who are looking for a new avenue to contribute is discussed in [6] through the wounded warrior project. The paper details the approach to digital forensics and investigation training at various levels from beginner to advanced. This work ties in closely with our own experience working our own cybersecurity training programs with wounded warrior. Using these works as a guide, we have worked to construct our program to most effectively teach the key concepts of digital forensics to interested students at both the high school level and above. Sources like [1] serve as a valuable reference to building the course material and adding technical details to the exercises to relate the to real-life examples.

There are numerous techniques that have been used to approach the idea of teaching and training in cybersecurity fields. These include using virtualization, cyber games and competitions, and more. The application of utilizing peer teaching to improve digital forensics education is detailed in [8]. The focus is on building the communication skills and the ability to articulate knowledge in practitioners of digital forensics. The idea is that investigators must be able to complete the technical work and then be able to support their analytical conclusions about a case. This is done by incorporating active collaborative learning to the teaching process. The development of cyber games for digital forensics education is a field of research that has grown significantly in recent years. It is a major focus in drawing more interest in many fields relevant to cybersecurity. The study in [18] proposes to use serious cyber games to promote active learning of digital forensics material and provides a proposed game to facilitate this active learning.

The concept of utilizing virtualization is considered in [9] [13] and [16]. Virtualization has made long distance learning a much more powerful and conceivable way to disseminate digital forensics training material. Advances in remote virtualization allows the instructor to provide greater support to the students and increases the possibility of collaborative learning between students. An original process for utilizing these remote virtualization techniques into a teaching process using remote desktops and applications is discussed in [16]. Virtual machines play no small part in the role that virtualization plays in the process of training and teaching students in digital forensics. The use of virtual machines has become pervasive in digital forensics education and [9] details a survey of student perceptions and opinions on the usage of virtual machines in undergraduate security courses.

Improvements have been made in the way of creating digital forensics curriculum and teaching approaches to establish program at various levels of education and difficulty of material. The University of Illinois at Urbana-Champaign details a new multidisciplinary undergraduate curriculum for digital forensics in [3] [11] and a thesis on the introductory course in [10]. The university developed a curriculum of lecture course at the introductory and advanced levels with appropriate parallel laboratory courses to reinforce the material. [3] details this curriculum along with the feedback of a workshop of digital forensics experts as to the merit of those courses. The current state of the program and the university's experience in trying to develop and teach the curriculum is provided in [11]. The introductory course curriculum and the progress made on establishing the multidisciplinary digital forensics courses is detailed in [10]. There is currently being no standard guide to designing digital forensics curriculum for academic programs and as such a great deal of work is being done to try and establish a baseline for these courses. To do this, [15] surveyed digital forensics educators and practitioners for the desired skills and knowledge needed and built digital forensics courses around them at the undergraduate and graduate level.

The implementation of hands-on learning methods has been instrumental to the training of new digital forensics professionals and students looking to pursue degrees and certificate programs in cybersecurity and digital forensics. A review of this hands-on discovery learning process is provided in [5]. The paper discusses discovery learning techniques and the level of success they have seen in incorporating information assurance topics in ABET accredited computer science and software engineering degree programs. It was found that students learned more and were more interested in learning when allowed to experience digital forensics concepts first-hand, as opposed to just hearing about them in lectures. It is important to look toward the future of the digital forensics field by focusing on how to approach teaching those are learning to be digital forensics practitioners now. [4] [14] take a look at the past ways to train digital forensics practitioners and the current state of training, education, certification, and accreditation of digital forensics programs.

The current state of professional certifications and standard bodies of knowledge used in education and training of up-and-coming digital forensics practitioners is examined and their impact on the discipline are given in these papers.

3. EXPERIENCE AND FEEDBACK

We have experience teaching digital forensics and cybersecurity concepts to different levels of students through programs such as wounded warrior, digital CSI summer camps at a university and forensics outreach program to a minority university. These workshops and summer camps serve as valuable data points for maintaining the courses that cater to novices and provides an educational and engaging experience to students ranging from computer novices to those more familiar with the operation of computers and other digital devices. We collect survey information from these projects in order to be constantly updated and adapting our material to make it better suited to dealing with the students that we target. We have a history of working with underrepresented communities, and can orient our program to maximize the impact it has on reaching out to these communities to create pathways for entry to science and engineering degrees. Some example feedback from students in the most recent summer camp held at the minority university showed good results for increasing knowledge about each of our core digital forensics concepts as well as an appropriate pace to keep students interested and engaged in the learning process. Some common trends in student comments have been:

- Slow down the pacing of the course
- More unguided hands-on practice to answer specific questions
- Some physical exercises with imaging and dealing with hardware
- More practical information
- Clarification of computer jargon and concepts
- Focus on introductory material for one-day workshops
- Different courses for beginners and advanced students
- Additional information and materials available online
- Mobile forensics hands-on examples

In response to these common trends from comments left by students, we have adapted the course material we have used and have made further improvements for the courses. The workshops will focus on a slower paced high level case study that presents an overview of material for a section before delving into more depth with the guided technical example. This process repeats several times over the course of the workshops. This allows the students to get the technical hands-on experience without getting left behind with the complex explanations of how everything works. The focus of the workshops is on a single device, a USB or hard drive, which has been imaged and can be analyzed. Both the workshops and the summer camp will have a more extensive introductory section that covers common computer jargon and will set the pace of the teaching based on responses from students. The summer camp serves the function of being the more advanced course where students would have ideally participated in the workshop, or have previous experience dealing with computers, but will not be necessary.

The summer camp will have more opportunities to allow the students to get some hands-on practical experience dealing with hardware for imaging and then analysis. The labs that are used for evaluation purposes in the summer camps satisfy the request for more unguided hands-on practice for the digital forensics concepts. The students will answer specific questions to reinforce the learning of the core concepts of each section of the course. The most recent trip to Western New Mexico University, in February of this year, saw the implementation of some of these changes with good results. The most recent set of surveys added the additional information about clarification of computer jargon and the students desire to obtain further educational material to work on their own, including mobile device forensics. This most recent set of feedback helped to lay the foundation for an advanced course that was requested by some of the students who are currently working in the field.

4. OVERVIEW OF COURSES

The courses we will discuss come in two main types: workshops and summer camps. The workshops are generally a one or two day course that focuses less on the details behind why different aspects of digital forensics work and why we use them and more on the hands-on exercises and leaving some lasting impression on the students about digital forensics. The summer camps, or any of our forty contact hour courses, use a more involved discussion and then exercise format that allows the students to learn a bit about why and how things are done, including some technical details, and then to experience those details firsthand with concrete case studies and labs. The forty hour contact courses last for a single week working eight hours a day and offer a college credit option depending on where we are teaching. Taking the course for credit allows us to involve those students more heavily in the learning process, completing additional assignments and tasks in order to evaluate them for credit and to get more involved feedback. What follows is our curriculum and general teaching strategies for both the short-term workshops and the longer summer camps.

4.1 Workshops

The workshops are generally the first point of contact with the students who participate in our courses. They differ from the summer camps which consist of forty contact hours with the students and are instead limited to a single day of content, possibly repeated more than one day to accommodate the number of students registered. This means that the content will be a more streamlined version of the introductory material that will be taught in the summer camp. The goal of the workshops is to appeal to the students with a very hands-on and involved series of exercises and discussions that will promote an interest in digital forensics and begin the student on a pathway to seek out science and engineering degrees and future courses with us. Using the feedback that we have gotten in the past from our numerous projects dealing with one-day workshops for varying levels of students, we have constructed a curriculum that allows for a high level of exposure to digital forensics concepts, while still letting the students get hands-on technical experience with a case study. This gives the students a baseline of information to work with when pursuing more information on digital forensics and gets them interested in the technical side through the hands-on demos.

The workshop walks the students through a single case study that encompasses all the major components that are taught in the longer summer camp, in some way. The students get a brief introduction to the digital forensics field and the environment that the work will be done in and then move right into the case study. The goal is to fit as much information into the workshop as possible, without overwhelming the students and causing them to get frustrated or confused. We will work at a high level and work our way to a more technical hands-on demo, before moving back up to the high level to begin the next phase of the workshop. For students who are interested in cybersecurity and digital forensics but have never had the chance to work on it before and are not confident in their computer skills, it can be overwhelming to give the students too much information too quickly. For that reason, we pace the workshops in a way that adheres to the knowledge level of the students while encouraging the students to work through the case study in small groups to aid in the understanding of the material. A sample schedule for a workshop is shown in Table 1.

Note that the timing is subject to change depending on the context of the workshop being taught. For a single day workshop that could be taught at a high school this is an appropriate schedule, but for a one-day workshop for professionals and college students, we cover an additional two hours of materials with a longer break in the middle of the schedule. The times in the table are subject to change depending on what the scheduling constraints of the high school are for lunch and students arriving and leaving school. It is possible that the course would go longer if in the registration we extend the time to $4:00$pm and ensure the students coordinate to get home from school in case they take the bus or someone has to pick them up. This initial schedule assumes the workshop would be taught during the school week, but after talking with the administration of the high school, it is possible that the course would be moved to a Saturday and the schedule could be adjusted accordingly and the fees for hosting the course would be covered in the proposal budget, i.e. lunch for students. A more detailed outline of the currently suggested workshop case study is detailed below. It is possible that the contents of both the workshop and the summer will change after any number of iterations based on student feedback and developments in the field of digital forensics.

During the course of the workshop the students will encounter many digital forensics and general computing concepts that are likely unfamiliar to them and are given the opportunity to experiment without risk using the provided laptops. The students will be exposed to working with virtual machines, command line operations and utilizing different guest operating systems, such as Kali Linux. The students are given a case study with an image file created beforehand of the suspect's digital device. With this image file we provide information about the suspect, suspected crime, description of the case and some examples of what type of evidence to look for. Using this model, we walk the students through the key concepts they will need to complete the case study and allow them to go about solving the case at each stage on their own, or in groups. The general series of steps taken by the students is as follows:

- Gain access through password cracking
- Create an evidence file in Autopsy
- Collect all evidence including hidden data
- Investigate the recovered evidence and registry data
- Learn about dealing with encrypted data
- Investigate image files using EXIF and steganography
- Present their evidence and analysis

4.2 Summer Camps

The summer camps are important for several reasons: a longer time spent with the students allows the instructors to go into more detail about digital forensics concepts, the instructor is able to build a rapport with the students which will encourage further communication from those that are interested, and the students are exposed to our university as an option for their undergraduate learning. The first point and most obvious is that the more time that the instructor spends with the student, the more material can be covered. As opposed to the workshops discussed previously, a summer camp allows the course to cover a greater depth of digital forensics material. The extended time also allows for more developed case studies for the students to experience and gives the students more time to process everything that they are learning. By spending more time with the students, a rapport is built which will cause the students to be more inclined to remain in contact if they are interested in learning more about digital forensics and our university. We have also found that students tend to give more useful and reliable feedback from the week-long courses. The curriculum for the summer camps is discussed below.

For each day, the instructor engages with the students in three ways: discussion, exercises and labs. The discussions take the form of an open-ended lecture where both high-level and technical detail will be explained to the students, who will be asked questions pertaining to the material and encouraged to ask questions about what they are learning. In the summer camps, we take advantage of the additional time with the students to begin introducing them to more detail than they have seen previously in the workshops, but without getting beyond the introductory level. The goal is to facilitate an understanding of the material and the technical concepts behind them without overwhelming the students with information that they will not understand or be able to properly process. That being said, if the students are interested in delving deeper into one of the particular topics, it is possible to set aside some time to do a more detailed version of any of the sections.

The exercises are guided examples that reinforce the information from the discussions. These are hands-on examples where the instructor helps the students to follow along and

Table 1: One-Day Workshop Schedule

Time	Concept	Action
8:00-8:55	Introduction	Review the environment
9:00-9:55	Command Line and Gaining Access	Command line and password cracking
10:00-10:55	Examining Evidence	Investigate target image
11:00-11:55	Persistence of Data and the Registry	Deleted data and the registry
12:00-12:30	LUNCH	LUNCH
12:35-1:30	Metadata and Encryption	File types and structures and encrypted data
1:35-2:30	Image Forensics	Steganography and EXIF data
2:30-2:45	Student Survey	Fill out survey

complete the tasks with the rest of the class. This gives the students some experience dealing with what they have just learned, and also serves as a reference point for the labs to be completed next. It should be noted that each discussion and exercise are meant to take approximately half an hour and the labs a whole hour. These times are flexible depending on how the students are understanding the material. More or less time can be spent on each portion as needed.

The labs are similar to the exercises because they are hands-on, but the students receive little guidance from the instructor. The intent of the labs is to have the students figure out the problems on their own, using the discussions and exercises as reference points to understanding how to complete the task. These labs serve as the primary means of measuring the students' understanding of the concepts being taught in the summer camp. It is important to get a clear measure of the merit of the teaching methods being used for the instruction of the high school students. The surveys taken by the students give an indication of their reactions and points of view on the course and the materials as a whole, but the labs serve as an appropriate evaluator of how much the students have learned. The summer camp curriculum sections are discussed in more detail below. An overview of the summer camp curriculum in table form is available in appendix A.

One thing to note about the students who take the summer camp or forty hour course for academic credit is that they must complete a project in addition to completing the course work. Our current students who took the course for credit in February were given an assignment to create a digital forensics exercise from the ground up. This is an ideal project for new students to work on because by creating the exercise themselves, they learn much more than by just doing the exercises we provide. An added benefit to this is that we can see what types of exercises the students find most interesting and utilize that information in future courses.

5. EVALUATING SUCCESS

The effectiveness of the courses are measured by student surveys and lab evaluations. The survey is done to measure the feedback of the students and obtain some information about the level of the students taking the courses. The lab evaluations serve to give concrete results as to how effective the teaching process is to introducing students to the concepts of digital forensics. This allows us to validate that all of our goals are being pursued and that we are making meaningful contributions to building effective courses for teaching each level of digital forensics that we offer. Some of the metrics that we measure are discussed here.

5.1 Demographics

With a large emphasis on outreach to minority and women for our courses, it is important that we accurately document who is attending the training sessions. This is key for measuring the interest the program has on increasing the number of minority and women applicants to cybersecurity degree programs.

5.2 Satisfaction Survey

This is completed by students to ensure that the level of education received through our course is satisfactory. This measures instructor preparedness, clarity, met expectations, future improvements, and other questions about the course itself.

5.3 Post-Course Survey

This is the other half of the survey that goes along with the satisfaction survey. In this survey the focus is on measuring the impact and effectiveness of each of the core digital forensics concepts that is taught in the course. It is important to measure the capabilities and knowledge of the students before and after completing the courses so that we can measure which sections may need more work and which sections are working well.

5.4 Lab Evaluations

The labs that are completed during the summer camps will be graded in the same way that a standard undergraduate course assignment would be. This is done to measure the academic results of teaching the students. Where the post-course survey and satisfaction survey measure the students reaction to the course and how much they feel like they have learned, the lab evaluations contain hard evidence of correct and incorrect answers to the lab tasks. Note that the grades here do not impact whether the students receive a certificate for completing the course, but are important for those students who are seeking academic credit for the course.

6. CONCLUSIONS

The relatively low cost of entry of digital forensics makes it an ideal pathway for students to become involved in cyber degree programs. Our courses lead to a measured increase in awareness in the students compared to what they knew of digital forensics and cybersecurity before taking the workshops or summer camp. One limitation to the current state of the courses is a lack of a permanent repository for placing our teaching material. It has already become much more commonplace to have freely available demos and how-to's on cybersecurity related blogs and websites. By using this trend to our advantage, we hope to soon make the dissemination of our digital forensics material free and open to the public, allowing a wider knowledge base among the populace. The limiting factors of time and money to learn the material will be somewhat alleviated by having a central repository for all of our digital forensics teaching material to allow a student to work through the material on the repository learning more about digital forensics for the first time, or an expert brushing up on some techniques and tools that they had not used in some time.

The impact of these outreach courses is important to facilitating an increase in students pursuing cybersecurity degrees. By targeting high school students in the summer before and during their senior year when they are making a major decision about where to attend university and what to major in, the number of students that will choose science and engineering fields will increase. By exposing students to digital forensics concepts who would not regularly have access to such material, we give the students an opportunity to engage in a field that they may not realize that they enjoy or are adept in. This impact also includes increasing the number of minority and women applicants to science and engineering degrees. In order to increase the number of minority and women in these fields you must engage them early in their academic careers and give them the opportunity to experience and become interested in cybersecurity fields. By using our experience teaching both high school students and professionals, we seek to create an effective and approachable curriculum for building interest in cybersecurity through digital forensics education.

7. REFERENCES

[1] B. Akhgar, A. Staniforth, and F. Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook.* Syngress, 2014.

[2] M. Al Falayleh. Building a digital forensic laboratory for an educational institute. In *The International Conference on Computing, Networking and Digital Technologies (ICCNDT2012)*, pages 285–293. The Society of Digital Information and Wireless Communication, 2012.

[3] M. Bashir, J. A. Applequist, R. H. Campbell, L. DeStefano, G. L. Garcia, and A. Lang. Development and dissemination of a new multidisciplinary undergraduate curriculum in digital forensics. In *Proceedings of the Conference on Digital Forensics, Security and Law*, pages 161–170, 2014.

[4] D. Dampier and J. Cohoon. Educating tomorrow's digital forensics examiners. *Innovations*, pages 273–282, 2008.

[5] D. Dampier and R. Vaughn. Hands-on discovery learning in computer security and forensics. In *Proceedings of the 2009 International Conference on Engineering Education and Research (ICEER), Seoul, Korea*, 2009.

[6] D. A. Dampier, K. Blaylock, and R. W. McGrew. Digital forensics workforce training for wounded warriors.

[7] K. Floyd and J. Yerby. Development of a digital forensics lab to support active learning. *DEVELOPMENT*, 4:14–2014, 2014.

[8] M. Govan. The application of peer teaching in digital forensics education. *Innovation in Teaching and Learning in Information and Computer Sciences*, (0):1–7, 2014.

[9] T. Imboden, N. Martin, J. D. Seib, and J. Phillips. Student opinion on the use of virtual machines in security education. In *Society for Information Technology & Teacher Education International Conference*, volume 2012, pages 3655–3660, 2012.

[10] A. Lang. A new portable digital forensics curriculum. 2014.

[11] A. Lang, M. Bashir, R. Campbell, and L. DeStefano. Developing a new digital forensics curriculum. *Digital Investigation*, 11:S76–S84, 2014.

[12] C. A. Lee and K. Woods. Digital acquisition learning laboratory: A white paper. *School of Information and Library Science University of North Carolina at Chapel Hill November*, 2011.

[13] V. Nestler and D. Bose. Leveraging advances in remote virtualization to improve online instruction of information assurance. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, pages 1–8. IEEE, 2011.

[14] M. Pollitt and P. Craiger. Educating the next generation of cyberforensic professionals. In *Advances in Digital Forensics X*, pages 327–335. Springer, 2014.

[15] M. Tu, D. Xu, C. Balan, et al. On the development of digital forensics curriculum. *Journal of Digital Forensics, Security and Law*, 7(3):13–32, 2012.

[16] R. Tuminauskas, D. Ambraziene, R. Miseviciene, and N. Pazereckas. Educational infrastructure using virtualization technologies: Experience at kaunas university of technology. *Informatics in Education-An International Journal*, (Vol11_2):227–240, 2012.

[17] R. B. Vaughn and D. A. Dampier. A university-based forensics training center as a regional outreach, education, and research activity. *Journal of Systemics, Cybernetics & Informatics*, 7(2), 2009.

[18] J. Yerby, S. Hollifield, M. Kwak, and K. Floyd. Development of serious games for teaching digital forensics. *Issues in Information Systems*, 15(2), 2014.

APPENDIX

A. SUMMER CAMP CURRICULUM

A.1 Monday Discussions

- D1.1 *Fundamentals*: An overview of the basic concepts of digital forensics including a review of hardware and software.
- D1.2 *VMs as Forensic Tools*: A discussion of what virtual machines are, how they work, and the role they serve in the field of digital forensics.
- D1.3 *Introduction to Cyber Crime*: A discussion of what constitutes cybercrime, current cybercrime trends, and why it is important to have people who specialize in pursing cyber criminals.
- D1.4 *Forensic Discovery*: The process for finding evidence on a digital system and how dealing with a digital

system is different from discovering forensic evidence in a non-cybercrime.

- D1.5 *Strings and Regular Expressions*: An introduction into the use of strings, and similar commands, along with regular expressions to search a computer for key words and phrases.
- D1.6 *Introduction to Command Line*: An introduction to the command line, how to use it, and why it is important to understand how it works.

A.2 Monday Exercises

- X1.1 *Learning the Environment*: A walkthrough of the virtual machines that will be used throughout the week to complete the digital forensics training and lab tasks.
- X1.2 *Password Cracking*: An example of cracking a Windows password to gain access to a device containing evidence that has been locked down.
- X1.3 *Google Hacking*: An example of how current and well-known tools can be subverted to allow a criminal to invade the privacy and confidentiality of others. Used to increase interest in cybersecurity concepts in the students.
- X1.4 *Learning the Command Line*: A series of exercises meant to reinforce the usage of the command line from the previous discussion.

A.3 Monday Labs

- L1.1 *Environment, VM, and Command Line*: An assignment where the student will complete tasks and answer questions about the testing environment, virtual machines, and command line.
- L1.2 *Password Cracking and Google Hacking*: Students will crack a password to a virtual machine image and access key data within the virtual machine. The Google web-searching system will be used to identify specified information and identify weakness in a target demo network.

A.4 Tuesday Discussions

- D2.1 *Disk Geometry*: The geometry of a hard disk is discussed, including how data is stored and retrieved, how a disk is broken into measureable pieces and what this means for locating evidence on a system.
- D2.2 *Imaging*: The process for imaging a disk or device is discussed along with why it is important to image devices and work on the image and not the original device.
- D2.3 *Hashing*: Different types of hashing algorithms are discussed and an overview of hashing is given. The focus is to ensure the students understand why hashing is important and why it is meaningful for validating digital evidence.
- D2.4 *Capturing RAM*: Read-only memory is discussed, particularly how to obtain information from RAM given that it is a volatile location for storing data.
- D2.5 *RAM Analysis*: A discussion on the implications of reading the data located in main memory and how to obtain that data.

A.5 Tuesday Exercises

- X2.1 *Collecting Evidence*: An exercise that combines parts of the previous discussions to detail the process for collecting evidence, including imaging and hashing the source data, and how to prepare that data for analysis.
- X2.2 *Examining Evidence*: An exercise that utilizes the SluethKit tool to take the image prepared in the previous exercise and investigates what information can be pulled from it and what the information means.

A.6 Tuesday Labs

- L2.1 *Evidence Gathering*: Students will repeat a process similar to exercise 2.1 except with new source data.
- L2.2 *Evidence Analysis*: Students will investigate the images that were created in the previous lab to identify key artifacts located in the image. Evaluation will be completed based on how many and which artifacts were located in the image, including questions that require the student to determine what was being done on the system.

A.7 Wednesday Discussions

- D3.1 *Persistence of Data*: The students will learn what happens to data when it is move to the trash and deleted or removedİ from the system in some other way.
- D3.2 *Data Erasure*: A more technical look at the way data is stored on the hard disk and what happens when data is deleted both on the operating system and the hard disk itself.
- D3.3 *Registry Analysis*: Students are exposed to the Windows registry and an overview of the registry and what it does is given.
- D3.4 *Browser History Analysis*: An example of how to use the registry to obtain information about the users on the system and attempt to understand how the system was being used.
- D3.5 *Metadata*: The content of individual files is discussed with a focus on metadata. Different types of metadata and how metadata can be used to aid in an investigation are discussed.

A.8 Wednesday Exercises

- X3.1 *Recovering Deleted Data*: A guided exercise on deleting some sample data and some data gathered by the students and having the students recover as much of that data as possible.
- X3.2 *Registry Examination*: An exercise that has the students investigate the registry to determine key factors, such as users, installed programs, password files, and others.
- X3.3 *Slack Space*: A walkthrough of what slack space is, how it is possible to store information in slack space, how to hide and recover data from slack space and how to detect data stored in slack space.
- X3.4 *Alternate Data Streams*: A walkthrough of what alternate data streams are and how it is possible to hide information in them. The focus of this exercise is to ensure students understand the differece between ADS and slack space and how different file systems can be exploited to allow for data to be hidden.

A.9 Wednesday Labs

- L3.1 *Locating Data*: Students will be given a virtual machine image and will investigate the image for any important data and answer questions, according to the sample scenario that accompanies the image. For example, an example investigation is discussed in the lab to give the students an idea of what type of evidence they would be looking for.
- L3.2 *Hidden Data*: Similar to the previous lab, students will be given a virtual machine image and are expected to use what they have learned up to this point to look for and identify any hidden data that would be useful to the given investigation scenario.

A.10 Thursday Discussions

- D4.1 *Reverse Engineering*: A high-level overview of what reverse engineering is and what role it plays in the field of digital forensics.
- D4.2 *Steganography*: The process for hiding data in .jpg, .png and other files is discussed here with an overview of the process and how it is used in cybercrime today.
- D4.3 *Encryption*: An overview of encryption methods and how encryption works is discussed, including common encryption methods, like TrueCrypt or BitLocker, and uncommon and simpler encryption algorithms used by the owner of a device to prevent a breach in personal security.
- D4.4 *EXIF Data*: The data type, where and how it is used is why it is important when dealing with image files located both on a subjects device and the web.

A.11 Thursday Exercises

- X4.1 *Steganography: Hidden Data*: An exercise on hiding data in image files, in addition to identify files with data hidden in them and how to retrieve that data.
- X4.2 *Dealing with Encrypted Files*: An exercise where students will encrypt and decrypt files and explore the differences in the files in their encrypted and decrypted form.
- X4.3 *EXIF Data Reading and Manipulation*: Students will collect EXIF data from files and then manipulate that data to obscure the capability of an investigator to utilize the data.

A.12 Thursday Labs

- L4.1 *Hidden Data II*: Building off of the previous lab 3.2, students will re-test their knowledge of hidden data on a system while investigating new possibilities for discovering hidden data through steganography and metadata, like EXIF.
- L4.2 *Dealing with Encrypted Data*: Students will tackle the problem of collecting meaningful evidence from files that are encrypted. Students will find ways to overcome the encryption using what was learned in the discussion as well as other evidence given in the assignment form.
- L4.3 *Evidence Analysis II*: The students will re-visit the TSK and Autopsy tool to analyze an image containing evidence found on a system. This time the evidence will include steganography, EXIF and encrypted data.

A.13 Friday Discussions

- D5.1 *Forensics Profession*: Students will learn more about professions that utilize digital forensics and how to prepare themselves to work in those fields.
- D5.2 *Network Analysis*: The analysis of network logs utilizing tools like Wireshark is discussed, as well as the implications of obtaining data from network traffic as opposed to off a subject's computer or digital device.
- D5.3 *Anti-Forensics*: Techniques and tools meant to disrupt the investigation of a device are discussed along with the process for overcoming them.
- D5.4 *Open Forum*: A section devoted to answering questions from students and discussing topics of interest.

A.14 Friday Exercises

- X5.1 *Email Spoofing*: Students will learn to spoof and email and to identify an email that has been manipulate in some way.
- X5.2 *Traffic Analysis with Wireshark*: Students will learn to investigate network logs and live network traffic in order to obtain evidence for their investigation.
- X5.3 *Dark Nets: TOR and I2P*: An overview of Dark Nets and the Deep Web, including metrics on internet use today, how distributed filesharing networks impact digital forensics investigations and what it means to be anonymous on the web.

A.15 Friday Labs

- L5.1 *Identifying Misdirection*: Using what they have learned from previous discussions and exercises, students will practice identifying misdirection in a device image. This will include differentiating between valuable evidence and fabricated and false evidence.
- L5.2 *Understanding Anonymity*: Students will explore TOR and I2P and answer questions about how anonymity works and what the potential impacts are for digital forensic investigations.
- L5.3 *Gathering Network Evidence by Utilizing Wireshark*: Students will analyze network logs and live traffic to answer questions about the test case that goes with the network logs and live traffic.