Digital Forensics Education Modules for Judicial Officials

Ragib Hasan[1], Yuliang Zheng[1], and Jeff Walker[2]

[1]Department of Computer Science
[2]Department of Criminal Justice
University of Alabama at Birmingham, Birmingham AL 35294, USA,
(ragib,yzheng,jeffw)@uab.edu,

Abstract. As our lives become more dependent on digital technology, cyber crime is increasing in our society. There is now an ever-increasing need to counter cyber crime through digital forensics investigations. With rapid developments in technology such as cloud computing, the Internet of Things, and mobile computing, it is vital to ensure proper training of law enforcement personnel and judges in the theory and practice of digital forensics. In this paper, we describe our methods and approach to create curricula, educational materials, and courses for training law enforcement and judicial personnel in digital forensics. We partnered with legal experts to design a series of modules/courses on digital forensics to educate the actual target demographics. Training materials have been designed to be not only scalable to nationwide law enforcement and judicial professionals, but also amenable to regular updates to respond to rapidly changing attacks and forensic techniques.

Keywords: digital forensics, education,

1 Introduction

In recent years, advances in computing has changed many aspects of our lives. The rapid growth of cyber technology has significantly improved different domains. However, at the same time, cyber crime is rising, leading to malicious use of computing technology. Prosecutors are increasingly relying on technology and digital forensics to investigate criminal activities. A report of the FBI states that, during the fiscal year 2012 alone, the Computer Analysis Response Team (CART) of the FBI supported nearly 10,400 investigations and conducted more than 13,300 digital forensic examinations that involved more than 10,500 terabytes of data [28].

The very nature of cybercrime and digital forensics is also changing as new technology is adopted by the society. For example, with the emergence of cloud computing, consumers are increasingly moving to the cloud for their storage needs. In 2012, Gartner predicted that consumers will store more than one third of their digital content in the cloud by 2016 [17]. By 2019, the use of clouds to store customer data has skyrocketed – a 2019 report by Gartner predicts

that "by 2022, 75% of all databases will be deployed or migrated to a cloud platform, with only 5% ever considered for repatriation to on-premises" [15]. Because of the large scale migration to the cloud-based storage and computation services, a large amount of forensic evidence is now derived from the cloud. Some incidents of storing contraband documents in cloud-based storage systems have already been reported [9,12]. Evidence residing on clouds has great impact on legal rules and regulations [8,14,21,25]. To prosecute and litigate a crime today, judicial officials therefore need detailed and advanced knowledge of computing, especially in the area of computer security and digital forensics. With rapid developments in technology such as cloud computing, the Internet of Things, and mobile computing, it is vital to ensure proper training of judges and prosecutors in the theory and practice of computer security and digital forensics.

Unfortunately, most of current cyber security and forensics education are geared towards technical experts or law enforcement investigators rather than judicial officials such as judges and lawyers. Most, if not all, of computer security and forensics educational material assume prior knowledge of computing and technology basics. People with a non-computer science background have difficulty in utilizing such educational materials to get a working knowledge of computer security and forensics. As a result, the judges and other officials have to blindly trust the experts associated with the trial, and assess the evidence with incomplete knowledge of the domain. The lack of domain knowledge in computer security and forensics technology can, and often does, lead to miscarriages of justice. Often, the digital evidence forms the core of a case and therefore the judges need to fully understand various aspects of the forensic evidence rather than completely relying on the expert witnesses. Therefore, there is a significant and urgent need for domain specific and appropriate computer security and forensics educational materials for judicial officials.

In this paper, we present an overview of our ongoing work to develop curricula, educational materials, and courses for training law enforcement and judicial personnel in digital forensics. We have created a set of educational modules and courses of various lengths that are geared toward judicial officials. To do so, we have partnered with judicial officials working in the area to develop and disseminate the courses and evaluate their effectiveness in educating the target demographics. We have also included mechanisms to frequently update the educational modules to match the rapid growth of technology. Our target audience includes judicial officials, including judges, prosecutors, attorneys, investigators, and other judicial personnel.

Contributions: The contributions of this paper are as follows:

1. We explored various aspects of legal cases and judicial processes to identify the specific domain knowledge that judicial officials require for learning forensics.
2. We developed domain specific and appropriate educational modules to teach computer security and forensics to judicial officials. The modules have been

designed to range from self-paced online courses to a single day short course, or a series of multiple courses to provide a comprehensive knowledge.
3. We also developed a continuous improvement process to evaluate and improve the effectiveness of various dissemination mechanisms to deliver the modules to judicial officials.

Organization: The rest of the paper is organized as follows: in Section 2, we provide background information on computer forensics and relevant laws. Section 3 provides motivation for creating this domain specific educational resource for judicial officials. We discuss the challenges of this work in Section 4. We provide details of our approach towards developing the educational materials in Section 5, and provide a sample module syllabus in Section 6. Finally, we conclude in Section 7.

2 Background

To provide the readers with an understanding of the scope of our work, we begin by exploring background information on computer forensics and the various laws governing the use of digital forensics in legal cases.

2.1 Computer Forensics

Computer forensics is the process of preserving, collecting, confirming, identifying, analyzing, recording, and presenting crime scene information. Wolfe defines computer forensics as "a methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format" [30].

According to a definition from NIST [19], computer forensic is "an applied science to identify an incident, collection, examination, and analysis of evidence data". In computer forensics, maintaining the integrity of the information and strict chain of custody for the data is mandatory. Several other researchers define computer forensic as the procedure of examining computer systems to determine potential legal evidence [20,23]. In recent years, the term Digital Forensics have become more widely used, since the forensic evidence can come from many electronic devices such as smart phones, GPS modules, etc., which are not usually considered as computers.

From the definitions, we can say that computer forensics is comprised of four main processes:

Identification: Identification process is comprised of two main steps: identification of an incident, and identification of the evidence, which will be required for successful investigation of the incident.

Collection: In the collection process, investigators extract the digital evidence from different types of media e.g., hard disk, cell phone, e-mail, and many more.

Additionally, they need to preserve the integrity of the evidence.

Organization:- There are two main steps in organization process: examination, and analysis of the digital evidence. In the examination phase, investigators extract and inspect the data and their characteristics. In the analysis phase, investigators interpret and correlate the available data to come to a conclusion, which can prove or disprove civil, administrative, or criminal allegations.

Presentation: In this process, investigators make an organized report to state their findings about the case. This report should be appropriate enough to present to the jury.

2.2 Legal Basis of Computer Forensics

We discuss the legal basis of computer forensics by discussing its use in criminal and civil litigation.

Criminal litigation: Digital forensics in criminal litigation is mainly governed by the 1986 Computer Fraud and Abuse Prevention Act. Subsequent court decisions such as Daubert vs. Merrell Dow Pharmaceuticals established the rules for admissibility of digital forensic evidence. According to the Daubert ruling, digital forensic evidence must be subject to the following standard [16]:

1. "Testing: Has the scientific procedure been independently tested?
2. Peer Review: Has the scientific procedure been published and subjected to peer review?
3. Error rate: Is there a known error rate, or potential to know the error rate, associated with the use of the scientific procedure?
4. Standards: Are there standards and protocols for the execution of the methodology of the scientific procedure?
5. Acceptance: Is the scientific procedure generally accepted by the relevant scientific community?" [16]

Civil litigation: In United States, before 2006, there was no separate US Federal law for computer forensics investigation in civil cases. As computer based crime was increasing rapidly, the Advisory Committee on Civil Rules took initiative to resolve this issue at 2000. In 2006, the Federal Rules of Civil Procedure (FRCP) provided the groundwork for the practice of electronic discovery in rule 26(a)(1)(A), which is known as e-discovery amendment [1] [18]. According to FRCP rule 34.(a), all Electronically Stored Information (ESI), including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations are subject to discovery by the litigating parties [2]. Transient data, including metadata, may also be considered as discoverable ESI [26]. Some important factors in the FRCP amendment, that are contributing in current digital forensics investigations are:

1. FRCP defines the discoverable material and introduces the term Electronically Stored Information (ESI). Under this definition, data stored in hard disk, RAM, or Virtual Machine (VM) logs, all are discoverable material for the forensic investigation.
2. It introduces data archiving requirements.
3. It addresses the issue of format in production of ESI. If the responding party objects to the requested format, then it suggests a model for resolving the dispute about the form of production.
4. It provides a Safe Harbor Provision. Under the rule of safe harbor, if someone loses data due to routine faithful operation, then the court may not impose sanction on him or her for failing to provide ESI [30,18].
5. A Litigation hold is known as a preservation letter or stop destruction request [26], which is introduced by this amendment. FRCP Rule 37 prevents an organization from removing documents from any of its storage system, which implies that ordinary data retention and cleaning policies should not be applied to ESI under a litigation hold [2,8].
6. There are also new and emerging challenges in forensics investigations in cloud environments [8,24].

3 Motivation

As we enter the third decade of the twenty-first century, there is an urgent need for training specifically for judicial officers. There are over 10,000 state and local judges in the US, and just under 3,000 federal judges. There are 2,300 prosecutor's offices at the state and local level, employing between 2 and 100 prosecutors. There are also 93 federal prosecutor's offices in the US, employing between 20 and 350 assistant prosecutors. This places the number of prosecutors between 5,000 and 20,000 prosecutors. With the increase in the involvement of digital evidence in both criminal and civil cases, it is likely many of these judges will have to rule on evidence of a digital nature in their cases. An October 2016 presentation from Joyce Vance, the erstwhile US Attorney for Northern District of Alabama, by 2020, almost all court cases would entail a cyber component [29]. The cyber component comes not only from the devices or computers used in the crime, but also to find more evidence and connections between various suspects.

The understanding required for judicial officials is different from that of law enforcement officers and investigators. Law enforcement must fully understand the technical aspects of computer forensic investigation. Judicial officials need a full understanding of the law related to digital evidence. These include the differences between digital and physical evidence under the law, potential negative influences on juries, how to address motions and challenges from both the prosecution and defense, and others. This means judicial officials need a different type of education related to digital evidence from those who conduct the investigations.

There are many computer forensic training courses for investigators, law enforcement officers, and students. For example, Zhang et al. have discussed digital

forensics education at the undergraduate level through the use of experimental learning techniques [31]. In 2007, Choo et al. identified the future need for educating judicial officials about digital forensics [10]. However, there are only a few training opportunities for judicial officials; thus the need for educational materials and training outlined in this paper. Of the courses that are offered for judicial officials, many of them are residential and for extended periods, from a few days to three weeks [3,4]. They are also sporadic or not offered on a national scope. As an example, Clancy et al. at the National Center for Justice and Rule of Law at the University of Mississippi have organized Symposiums on the search and seizure of electronic information [11]. However, the main focus of these series of symposiums was on the seizure of information and 4th amendments. There is a need for a workshop focusing on all aspects of digital forensics.Finally, the number of judges and prosecutors that need this kind of training rapidly overwhelms current training options. Our current work would augment these courses and create a broader spectrum of courses available to judicial officers that would greatly improve their understanding of this areas. The increased understanding would provide for better legal decisions.

3.1 Differences Between Computer Forensics and Other Legal Issues

Computer forensic issues in court are complex and continually changing. Further, computer forensic issues have become a part of the procedure of criminal prosecution, not simply a point of fact. As a result, judges and prosecutors have to have a thorough understanding of computer forensic issues related to law. These involve, but are not limited to, seizure of digital evidence (computers, cell phones, GIS data from a variety of devices, social media information, etc.); how digital media is searched, stored, and presented in court; Fourth Amendment issues of rights to privacy; and a host of other computer forensic issues that may come up in a court proceeding.

What was once documents that were tangible artifacts (pictures, letters, contacts, etc.) when the Fourth Amendment was created are now almost universally contained in a digital environment. This represents the greatest challenge to the Fourth Amendment in the history of the US. As pointed out in Riley v. California [7], many of the issues faced by judges and prosecutors did not even exist with the Fourth Amendment was written. Not only must judges and prosecutors be trained in computer forensic issues, they must also continually update their training. Cyber security and cybercrime evolve so quickly, that their knowledge may be outdated within a few months.

Furthermore, judges cannot simply rely on expert witnesses as they have in the past. In many areas, such as medical procedures, there is a specific issue that must be addressed in the court proceedings (such as the effect of a drug or a cause of death). That is not the case for digital evidence, however. There is a much broader issue of this kind of evidence in the court proceedings. To allow a forensic examiner or an expert witness to serve as the source of knowledge in the digital evidence would be tantamount to allowing police officers to determine if a search

was within the Fourth Amendment. Judges and other judicial personnel need a much better understanding of computer forensic issues and digital evidence.

3.2 Difference Between Training Judges and the Police

There is a great deal of training in computer forensics for police officers; but much less so for judicial officials [22,13]. There is also a significant difference in the kind of training necessary. Training for police officers is one of two types. The first is technical aspects of digital evidence. First, officers need to know how to safely and legally seize digital evidence and how to process it. This is very technical, hands-on training. Second, police officers need to know what the law says and how to work within the law. This is application of legal issues, where officers merely need to know what the law is and how they must act to comply.

Judges, however, are making the law. They must interpret the legal standards that have been set in higher courts; but, in the rapidly changing environment of computer forensics, this is not an easy task. Historically, application of the Fourth Amendment was fairly straight forward. There was a seizure of a tangible object (a letter, drugs, etc.). It was then a matter of interpreting the legal precedent related to seizures. This is completely different for digital evidence. First, there is the issue of whether information stored electronically is even physical evidence that falls under the Fourth Amendment. This is much more difficult than it sounds because, as soon as the law establishes the parameters for digital evidence in one device, technology changes and renders previous decisions moot (such as the difference between files stored on a hard drive and files stored in the Cloud). Judges must react to these changes within the short time frame of a trial, where interpretation of previous law may not be clear. For this reason, judicial officials need a strong training program so they can understand both the technical aspects of computer forensics and the legal issues and background. Also, this training must be ongoing to address the continual changes both in law and in technology.

3.3 Lack of Proper Understanding of Digital Evidence May Lead to Miscarriages of justice

An example of the potential for miscarriages of justice related to digital evidence can be found in the 2014 Supreme Court case of Riley v. California, 134 S. Ct. 2473 (2014) [7]. In that case, Riley was stopped and suspected of weapons violations. After arrest, officers searched Riley prior to moving him to pretrial detention. During an inventory of Riley's possessions, an officer accessed his cell phone and went through the information. One item the officer found was repeated use of a term that was related to a street gang. Riley's phone was examined at least one other time by officers. Based on the texts and images found on the phone, Riley was charged in connection with a recent shooting. At trial, Riley argued that the cell phone was protected under the Fourth Amendment, and that it should not have been searched without a warrant specifically connected to the shooting. The trial court denied the motion and Riley was convicted and sentences to up to life in prison.

The California Court of Appeals affirmed the conviction, relying on a previous ruling (People v. Diaz [6]), which had held that searches of cell phones by police were admissible in court if they were retrieved directly from the person arrested. However, the U.S. Supreme Court overturned the conviction. In its ruling, the Court ruled that, in its current state (as differentiated from previous cell phones that only served as phones) a cell phone was "not just another technological convenience" and that it holds the "privacies of life" (pictures, addresses, documents) that deserve the protection of the Fourth Amendment. In this case, the Court rejected a precedent that dealt with officer safety and destruction of evidence because the cell phone in this case was in the possession of the police and not accessible by Riley. The Court left open what it would rule in the case of a cell phone that a subject might be able to get to to destroy evidence. The Court also left to future decisions whether accessing information that might be relevant to officer security (such as a text that the suspects confederates were headed to the scene to attack officers). The Court also wrestled with the difference between what officers are allowed to do in relation to seizures of physical evidence compared to digital evidence. This is something that will continue to be addressed in future cases. Finally, the Court discussed but did not rule on issues of the potential of another person to remotely wipe a cell phone and whether that would result in a need for officers to access and even forensically copy a cell phone. In this case, there were a number of hypothetical situations addressed; however, the Court chose to focus only on the narrow issue of the search of a cell phone related to an inventory search of an incarcerated person. This leaves open many issue that courts will have to wrestle with on an almost daily basis – it shows the potential for miscarriages of justice if courts do not make the proper interpretation, shows how important it is for judicial officials to have quality training in legal issues related to computer forensics, and demonstrates that this training must be continually updates so judicial officials understand both the technological advances and changes in legal thinking.

4 Challenges

Providing computer forensics education for judicial officials face several challenges.

4.1 Scope and Depth of the Curriculum

Computer security and digital forensics have become a very large field of knowledge. Judicial officials need to understand the latest techniques used in cybercrime investigations. However, currently available educational material and courses in security and forensics often requires technical knowledge of computing, which is outside the expertise of most judicial professionals. Therefore, the curriculum needs to provide in-depth coverage of the latest topics of computer security and digital forensics while not requiring deep technical expertise. The challenge is to determine the scope and depth of the curriculum and to present security and forensics concepts at the level understood by judicial officials.

4.2 Designing a Domain-Specific Curriculum

The curriculum also needs to be highly domain-specific. Many concepts in computer security and forensics are addressed and understood in different names and terms in the judicial/legal domain. Also, many terms used in court proceedings have unique and specific meanings which may not be obvious to computer science and forensics educators. Therefore, it is important to explain various security and forensics concepts using the terminology used in the legal profession.

4.3 Time Constraints for Education

Judicial officials such as judges are extremely busy. Therefore, the courses and modules need to be short enough so the target demographics can afford to set aside time to explore the modules. For example, most if not all judges will not be interested in a semester long course, but may have time for a few days of training in digital forensics and computer security.

4.4 Finding the Best Dissemination Mechanism

The curriculum should be flexible enough to be taught in-class, through correspondence, or via online. Finding the best possible dissemination mechanism is one of the objectives of this work.

4.5 Keeping the Content Up-to-Date

The field of computing changes rapidly. Therefore, it is essential to keep the material up to date. However, updating the course content especially the videos is difficult and time-consuming. To complicate the matter, to add new content to the video resources, it must be consistent with existing videos (e.g., taught by the same instructor, or in the same format).

4.6 Scalability

The biggest challenge is scalability. There are tens of thousands of judges and judicial officials in the US. Teaching them on-site in any one or a few particular locations is not feasible. However, the curriculum is vital for the entire community of judicial officials. Therefore, we must determine a way to scale the curriculum so that it can cover the entire community of judicial officials.

5 Approach Towards Developing the Educational Materials

To develop develop educational material for judicial officials and overcome challenges stated in the previous section, we took a multi-step approach involving a set of tasks, starting with requirements analysis for educational material, design

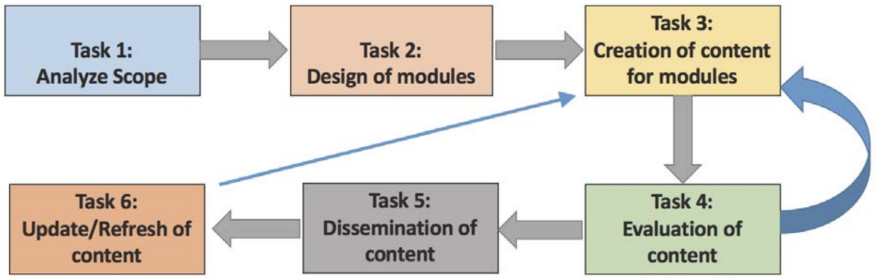

Fig. 1: An overview of the workflow for generating the educational modules

of customized modules, creation of the modules, the evaluation and dissemination of content, and periodic updates which focus on scalability and replicability. An overview of our workflow is shown in Figure 1.

Next, we discuss each of the tasks in detail.

Task 1: Analysis and customization of educational materials for use by judicial officials In this task, we analyzed and customize educational materials for use by judicial officials. The task involves two parts: collection of computer forensics educational material and discussion with judicial officials and justice sciences researchers to identify topics relevant and appropriate for judicial officials.

The goal of this task was to identify the subset of computer security and digital forensics educational material is relevant in the context of educating judicial officials.

Process: This phase was conducted in close collaboration between UAB's Computer Science and Criminal Justice departments. We have conducted meetings with judicial scholars to explore the research domain and create a set of topics that will be relevant to educate judicial officials. We also worked with lawyers to identify the topics.

Result: From Task 1, the result was a list of topics in digital forensics and computer security, ranked based on their significance. Also, we identified a list of foundational topics (i.e., basic terminology and concepts) that judicial officials without a technical background would need to know.

Task 2: Designing a set of modules with different paces and learning curves Different judicial officials have different time constraints; therefore, we must create a flexible range of modules to suit all types of schedules. In this task, we created a set of educational modules with similar/overlapping curricula, covering digital forensics and computer science at various degrees of depth.

We have created multiple sets of modules at different levels. For example, this includes: 1) A one day crash course on digital forensics 2) A set of multiple

day and multi-lecture modules for deeper exploration of computer forensics, 3) A set of self-paced learning resources which judicial officials can consult at their own time, and 4) a mobile and web app for quick reference.

The goal of this task was to determine the optimum set of modules to provide the best possible knowledge dissemination for a major portion of the target demographics of judicial officials.

Process: To determine how many different type of modules have to be prepared, we explored similar resources in other domains to get an idea of the best practices.

Results: The deliverable from this task were a set of module tracks, with various durations and depths, and a complete syllabus for each of the modules.

Task 3: Use of video and multimedia technology to create modules In this task, we created educational materials for the modules. This included development of video, web, and print materials to be distributed to the judicial officials.

The goal of this task was to determine the following (a) What is the best way to disseminate content to the target demographics? (b) What length of videos would be most preferred by the judicial officials?

Process: We used the following process to create the content:

- Video: For each module, we identified discrete topics and concepts covered by that module. We broke down the content into small chunks and short videos (5-10 minutes) on each topic. Breaking videos down to short chunks has several advantages: each chunk is easy to update without requiring edits to other chunks; short videos are also preferred by viewers when viewed online. Topics are relatively independent of one another to increase their chance of reuse in different modules. For the videos, we used both a classroom-based scenario (an instructor giving a lecture in front of a whiteboard) and a slide-based scenario (slides with narration), and a combination. We prepared the video lectures in accordance to the Quality Matters rubric for effective online courses [5].
- Text: We also created brief description of each topic along with examples. For each module, we prepared a short workbook.
- Web: Both the video and text material for the modules are hosted on a server to make them accessible to the target audience.

Results: The result from Task 3 were (a) a set of print materials, example problems, evaluation quizzes, (b) a set of videos covering various topics in the modules, and (c) a website hosting the modules and related links.

Task 4: Evaluation of the quality of modules The goal of this task is to determine the quality of the educational material developed for this project and whether this will be effective for optimal dissemination of knowledge to the target demographics.

Process: In this ongoing task, we are working with UAB's Center for Educational Accountability (CEA) to evaluate the quality of the educational materials. The CEA evaluates a range of education, health, and training (e.g., combat casualty training) programs.

The basic evaluation model to be used with this project is the Context, Input, Process and Product (Outcome) or CIPP evaluation model [27]. In this model, the context and input evaluations are designed for assessing the planning of the project and interpreting results, whereas the process and product evaluations are designed for assessing the implementation and outcome of the project.

Additionally, we plan to work with an educational consultant to evaluate the courses for Quality Matters (QM) certification [5]. We are also planning to make extensively use the IDEA survey of course participants to get feedback about the course.

Task 5: Dissemination of modules to target demographics In the ongoing Task 5, our goal is to explore different ways to disseminate the content to the target demographics. The various technique we have explored or plan to explore includes workshops offered at UAB Criminal Justice department, workshops at various state and national legal conferences for judges and prosecutors, partnerships with forensics standards bodies and organizations, through the website prepared in Task 3, and through a mobile app created especially for judicial officials.

Through these activities, we plan to determine the optimum, cost-effective, and most scalable method to disseminate the educational material to the target demographics.

Task 6: Periodic update and refresh of modules Here, we have identified the best practices for regularly updating and refreshing the module with new knowledge of technology used in digital forensics.

The goal of this task is to determine how we can keep the content up-to-date when the technology changes rapidly.

In accomplish this, we have developed a mechanism for efficient periodic updates to the modules. Technology changes rapidly, and we assume that we will have to update the content every year or every two years in order to provide an updated and current understanding of security and forensics. To do that, we have developed following workflow:

- During the update-review period, we will consult domain experts to determine whether the content is current and up-to-date.
- We will also crowdsource the analysis of the relevance of the modules by inviting the general judicial community to explore our modules and suggest changes.
- At the end of the review period, we will collect all the suggestions both from the experts and the crowd to determine which portions of the modules will require a change.

- We will then re-shoot the video segments, if possible with original narrators or teachers, and update the content. For new content, we will add them to the module repository. Also, the text content of the modules and the syllabus will be updated accordingly.
- For our mobile app, a push-notification will be sent to the mobile app to notify the user regarding the update to the content.

6 Sample Syllabus from the Educational Materials

Here, we provide a sample syllabus from one of our modules to demonstrate the structure of our educational materials.

Module 101: A One-Day Module on Computer Security and Forensics for Judicial Officials

Total hours: 5 hours
Syllabus:

1. **Hour 1**: Basic security building blocks and terminology, common attacks, common defensive measures
2. **Hour 2-3**: Computers forensics, tools, steps, terminology, reporting rules, laws regarding computer forensics and digital evidence
3. **Hour 4**: Security and forensics in emerging technologies such as clouds, Internet of Things, mobile devices (smartphones, notebooks, tablets)
4. **Hour 5**: Discussion/Q&A/best practices/review

This module has been created for both an in-class and an online audience. For the latter, each hour has been broken into many video units, with each unit discussing a separate topic/concept. The last hour of discussion and Q&A for online students is done in the flipped mode, where an online live session is arranged monthly using Google Hangout.

7 Conclusion

In today's world, almost every aspect of our lives increasingly involves the use of computer technology. It is therefore imperative to educate the judicial officials about digital forensics process and best practices. In this paper, we have presented our approach towards creating a set of scalable and sustainable educational materials for teaching digital forensics to judicial officials.

We posit that the presence of such a set of educational materials would be highly beneficial to ensure proper education of judicial officials, which will lead to better and informed prosecution of legal cases. Educating the law enforcement

and judicial personnel would allow them to understand and handle the increasingly omnipresent digital forensic evidence in legal cases and investigations. This would lead to significant improvements in investigating and prosecuting cybercrime, leading to a safer society for all.

8 Acknowledgements

This research was supported by the National Science Foundation through awards DGE-1723768, ACI-1642078, and CNS-1351038.

References

1. Federal Rules of Civil Procedure Rule 26., https://www.law.cornell.edu/rules/frcp/rule_26
2. Federal Rules of Civil Procedure Rule 37, https://www.law.cornell.edu/rules/frcp/rule_37
3. National Computer Forensics Institute (NCFI), Courses, Available at, https://www.ncfi.usss.gov/ncfi/pages/courses.jsf
4. National District Attorneys Association, Digital Technology Training, http://www.ndaa.org/digital_technology_training.html
5. Quality Matters Rubric, https://www.qualitymatters.org/why-quality-matters/about-qm
6. People v. Diaz, 51 Cal. 4th 84, 244 P. 3d 501 (2011)
7. Riley v. California, 134 S. Ct. 2473 – United States Supreme Court (2014)
8. Araiza, A.G.: Electronic discovery in the cloud. Duke L. & Tech. Rev. p. 1 (2011)
9. BBC, Lostprophets' Ian Watkins: 'tech savvy' web haul (December 2013), http://www.bbc.com/news/uk-wales-25435751
10. Choo, K., Smith, R., McCusker, R.: "future directions in technology-enabled crime: 2007–09.". "Research and public policy series no. 78. Canberra: Australian Institute of Criminology" (2007)
11. Clancy, T.K.: National center for justice and the rule of law. Online at https://olemiss.edu/depts/ncjrl/index.html (2004-2014)
12. Dist. Court, SD Texas. Quantlab technologies ltd. v. Godlevsky. Civil Action No. 4: 09- cv-4039: (2014)
13. Dotzauer, E.: COE - Cybercrime Training for Judges and Prosecutors: a Concept
14. Dykstra, J., Riehl, D.: Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing. Rich. JL & Tech. 19, 1 (2012)
15. Feinberg, D., Adrian, M., Ronthal, A.: "the future of the dbms market is cloud". Online at https://www.gartner.com/document/3941821 (2019)
16. Garrie, D.B.: Digital forensic evidence in the courtroom: understanding content and quality. Nw. J. Tech. & Intell. Prop. 12, i (2014)
17. Gartner Inc.: Gartner says that consumers will store more than a third of their digital content in the cloud by 2016. (2012), https://www.gartner.com/newsroom/id/2060215
18. K & L Gates: E-discovery amendments to the federal rules of civil procedure go into effect today (December 2006), http://www.ediscoverylaw.com/2006/12/articles/news-updates/ediscovery-amendments-to-the-federal-rules-of-civil-procedure-go-into

19. Kent, K., Chevalier, S., Grance, T., Dang, H.: Guide to integrating forensic techniques into incident response. NIST Special Publication 10(14), 800–86 (2006)
20. Lunn, D.: Computer forensics–an overview. Sans Institute 2002 (2000)
21. Nicholson, J.A.: Plus ultra: third-party preservation in a cloud computing paradigm. Hastings Bus. LJ 8, 191 (2012)
22. Proia, A.A., Simshaw, D.: Cybersecurity and the legal profession. Cybersecurity in Our Digital Lives 2, 119 (2015)
23. Robbins, J.: An explanation of computer forensics. National Forensics Center 774, 10–143 (2008)
24. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud forensics: An overview. 7th IFIP International Conference on Digital Forensics (2011)
25. Smith, J.: Electronic discovery: the challenges of reaching into the cloud. Santa Clara L. Rev. 52, 1561 (2012)
26. Stacy, S.: Litigation holds: ten tips in ten minutes (2014), https://www.ned.uscourts.gov/internetDocs/cle/2010-07/LitigationHoldTopTen.pdf
27. Stufflebeam, D.L.: The cipp model for evaluation. In: International handbook of educational evaluation, pp. 31–62. Springer (2003)
28. The Federal Bureau of Investigation: Piecing together digital evidence (2013), https://www.fbi.gov/news/stories/2013/january/piecing-together-digital-evidence
29. Vance, J.: Partnering with the U.S. Attorney to Fight Cyber Crime. Cyber 2020, University of Alabama at Birmingham (October 2016)
30. Wiles, J., Cardwell, K., Reyes, A.: The best damn cybercrime and digital forensics book period. Syngress Media Inc (2007)
31. Zhang, X., Choo, K.K.R.: Digital Forensic Education: An Experiential Learning Approach, vol. 61. Springer (2019)