Journal of Information Technology Education:
Innovations In Practice

Volume 12, 2013

Digital Forensics Curriculum in Security Education

S. Srinivasan
Texas A and M International University, Laredo, TX, USA

srini@tamiu.edu

Executive Summary

Information Security curricula usually cover traditional security topics such as network security, cryptography, and operating system security. As individuals and businesses have come to rely more heavily on computing technology, criminals also have turned their attention to such technology. Consequently, security requires developing adequate policies to protect the information assets, as well as gathering suitable evidence in case the matter ends in a court. Rapid advancements in storage technology have contributed to storing large volumes of data in small devices. Such devices could be hidden with criminal intent or are prone to being lost, thus exposing confidential information. In either case, we need to expose the students specializing in security education to both the technology and the legal aspects.

The author had the benefit of working closely with Information Security educators in the nation as part of the National Security Agency effort to develop curriculum that will address the security needs of the United States. In this regard the author developed a course in Digital Forensics as part of an Information Security Curriculum. When presentations were made in regional conferences about these efforts, the author found out that there was faculty in other institutions who were interested in starting a similar course in their institutions. They were also faced with similar financial challenges in developing a dedicated lab for Digital Forensics. Having taught this course twice, the author had ferreted out and obtained many inexpensive software packages to support the digital forensics curriculum.

In this paper, the author will share a sample undergraduate curriculum, resources needed to develop an inexpensive digital forensics lab, and steps to integrate this course in the InfoSec curriculum. As a motivation for this approach, first a brief history of Digital Forensics investigative history around the world is presented. This discussion identifies the major organizations that have contributed to the development of the necessary standards. The section on curriculum lays out the core learning objectives and the course content needed to cover these objectives. This is followed by details on setting up a Digital Forensics Laboratory. In this section, the author points out the usefulness of collecting hard drives from old computers and also the need to have several old computers available for teaching about the hardware elements. The section on Resources lists numerous free software resources as well as the ability to obtain commercial grade software from Access Data Corporation for free for instructional purposes. One of the key requirements in a digital forensics investigation is safe handling of evidence. This aspect is emphasized in detail about the Chain of Custody for data and presentation of

Editors: Beth Thomsett-Scott and Linda V. Knight

evidence analysis to a court of law. The paper is concluded with lessons learned as well as what the next steps would be for future enhancements.

Keywords: digital forensics, curriculum, tools, security, evidence, data hiding, computer crime

Introduction

The use of computers is growing rapidly. For many years, the emphasis has been upon storing computerized data in a structured way so that the data could be retrieved readily when needed. Today we are able to capture data easily from places as diverse as points of sale and manufacturing centers. Because of the tremendous volume of data available today, search technologies have become popular to facilitate data retrieval from any stored place. This positive feature has also become a drawback, as people with criminal intentions are able to locate more information with ease.

The major types of computer crimes committed could be classified as:

- White-collar crimes (computers used to store and manipulate data, remote access)
- Violent crimes (premeditated planning using computers)
- Terrorism (planning, communicating and gathering intelligence about the target using computers)
- Espionage (surveillance and communication using computers)
- Counterfeiting (planning and design using computers)
- Drug trafficking (management of database of customers, suppliers, and financials)
- Pornography (storage of large volumes of video and photos in digital devices)

In criminal investigations, law enforcement often seeks the expertise of digital forensics examiners to inspect confiscated computer systems for evidence. For example, people involved in child pornography may create their videos using other devices but store their work in computers, hiding these files from discovery using ordinary tools. Thus, computer crime should not be thought of as one involving computers exclusively but also as one where computers are used as an accessory or tool. We use this broad definition here in discussing computer crimes.

The modes of computer usage in crimes could be described as:

- Target of crime (e.g., ATM machines)
- Instrument of crime (e.g., Internet fraud)
- Information repository for crime (e.g., money laundering schemes)

Investigating computer crimes and presenting evidence in a court has become an important tool in fighting such crimes. This field of investigation has come to be known as computer forensics. Today, given the growth of technology, people are using a multitude of digital devices, not just computers, to facilitate communication and commerce. As such, the study of Computer Forensics today is heavily involves the realm of, Digital Forensics which includes all forms of digital storage and retrieval. This new discipline is defined in various ways by different people. For our purposes we will use the following working definition adapted from Lunn's work: Computer Forensics involves the preservation, identification, extraction, and documentation of computer evidence so as to present in a court (Lunn, 2001).

Digital Forensics evolved as a discipline only within the past 20 years. To understand the beginnings of this discipline Whitcomb provides an excellent historical account (Whitcomb, 2002).

For many years, computer forensics was primarily done by law enforcement, and courts treated evidence generated by forensic investigations similar to the way they treated physical evidence. The FBI created the first systematic investigative team, called the Computer Analysis and Re-

sponse Team (CART), in 1984. In 1993, the FBI organized the first International Conference on Computer Evidence. This conference was attended by representatives from federal, state, local, and international law enforcement agencies. Participants agreed that there were no formal standards for this forensics area. Consequently, follow-up conferences were held in U.S. in 1995, followed by similar conferences in Australia in 1996 and the Netherlands in 1997. This series of conferences eventually led to the formation of the International Organization on Computer Evidence (IOCE), which is plays a major role today. Even though CART and other FBI activities were instrumental in sowing the seed for the formal discipline of Computer Forensics, an FBI survey in 1995 showed that 70 percent of all investigative agencies were doing computer forensics work without a formal procedures manual. The IOCE, the FBI, and others have contributed to developing common standards for forensics examination. Much of the initial work in this area was done by Mark Pollitt and his associates (Noblett, Pollitt, & Presley, 2000). In spite of this progress, there still is no single recognized certification for forensic examiners. Yet, since one of the goals of digital forensics is to generate evidence for presentation in a court, having accepted norms is important for such evidence to be given appropriate weight.

As discussed above, the IOCE's efforts in developing common standards for computer forensic investigation around the world has been significant. In 1997, the IOCE issued a call for standards in gathering evidence. This was followed by a communiqué from the 1998 G8 summit emphasizing the need for international standards to combat computer crime. This resulted in the IOCE developing a standard and presenting it to G8 in 2000 (G8 Summit, 2000). One of the main contributions of this standard was in guiding a variety of groups, including first responders, to follow acceptable standards in gathering evidence. In the U.S., Regional Computer Forensics Laboratories (RCFL) were created by the FBI to support investigating computer crimes (RCFL, 2013). At present there are 16 RCFLs in the U.S. In order to exchange ideas among computer forensic investigators, besides the IOCE, the following three associations are making significant contributions:

- International Association of Computer Investigative Specialists (IACIS)
- High-Technology Crime Investigation Association (HTCIA)
- Computer Technology Investigators' Network (CTIN)

The discussion so far has been focused on explaining the development of digital forensics as a discipline. In the past, this field received the attention of law enforcement only. Over the past five years, this field has received increasing attention from academic institutions in the U.S., particularly Community Colleges. The importance of including Digital Forensics as a subject in an academic curriculum was articulated in papers by Yasinsac and Manzano (2001) and Yasinsac, Erbacher, Marks, Pollitt, and Sommer (2003). Yasinsac used the terminology Computer Forensics, which is subsumed by Digital Forensics. Chi (2009) presented details on the development of a laboratory for teaching Digital Forensics to undergraduate students. Interest in teaching Digital Forensics as part of the academic curriculum is prevalent in Europe, Australia, and Africa as well. We briefly present the details from published literature on Digital Forensics from these three continents. Anderson and his co-authors (2005) present details on their German and British experience in offering computer forensics courses. Their research indicates that in Britain the focus is on educating students "in using standard forensic tools, whereas the German case is more aimed at training students to build and improve standard tools." In the case of Australia, Lim (2006) points out the need for more computer forensics trained students. Lim's paper describes a six-dimensional knowledge model for computer forensics that deals with "categories of crime, computer technology, security, legislation, investigation process, and forensic tools." Stander and Johnston (2007) analyze the need for forensics curriculum in South Africa. They point out that types of computer crimes include hacking, denial of service, virus attacks, identity theft, cyber bullying and intellectual property theft. In their curriculum they introduce the concept of "End-to-

End Digital Investigation process," which includes all the traditional steps discussed later in this paper. Two other useful references based on US experience are the work of Austin (2007) in which he identifies several inexpensive tools to teach Digital Forensics and Batten and Pan (2008), who discuss their experience in teaching Digital Forensics at the undergraduate level.

The author has had the opportunity to develop and teach Digital Forensics as part of the Information Security undergraduate curriculum twice in the past three years. The course focuses on portraying the essential requirements needed to (1) monitor defenses set up for protecting networks and (2) bring any perpetrators of computer crime to justice. Toward this goal, the computer scientist must be aware of the legal requirements for obtaining, preserving, and presenting such evidence in a court. Such legal requirements are a necessary part of the course. At the author's institution, ethics topics are integrated in multiple courses. Consequently, many of the legal aspects associated with ethical situations, such as posed by Smyth v. Pillsbury (Standler, 1998), are covered in this course.

We are pleased with the success of this course. Our student survey for the course asked the students to rate the course's usefulness for understanding security issues. More than 80% of the students rated the course as very useful for their understanding of the security issues.

The sections below describe what has worked as an academic curriculum, how we constructed a laboratory with minimal cost, our lessons learned, and how other institutions might benefit from our experience.

Curriculum

Digital Forensics is offered as one of the five courses in an Information Security concentration in the Computer Information Systems undergraduate program. We offer this course in alternating years. A similar course is also offered in the Computer Science Masters program periodically. First, this course is enabling the InfoSec concentration to offer a total of five courses from which the students can choose four courses to meet the concentration requirements. From a curriculum perspective, this course gives the students an exposure to hardware aspects and teaches them how to use certain investigative tools and how to gather as well as protect evidence. We developed this course with help from Purdue University's Information Security program where multiple courses are offered in Digital Forensics in their Technology program. The first time we taught this course we offered a one credit course titled "A+ for Forensics." This course helped us build the necessary lab exercises and obtain the necessary laboratory resources, which we will describe later in this paper. We used this one credit course as a pre-requisite one time for the Digital Forensics course. Afterwards, we found out that it would be better to incorporate much of the content in the regular course in Digital Forensics, thus removing the pre-requisite. The course objectives we had were as follows. These are presented in line with Bloom's Taxonomy. Upon completion of the course the students would be able to:

- Describe the basic concepts of Digital Forensics.
- Explain the ways of gathering evidence.
- Explain the legal constraints of evidence collection.
- Show the implications of data access, storage and data hiding techniques.
- Differentiate data recovery methods using multiple storage devices.
- Compare the implications of privacy laws in the forensics context.
- Analyze the ethical aspects in dealing with Computer Forensics.

In trying to accomplish these course objectives we identified the following topics for the course:

- Introduction to Digital Forensics
- Computer Investigation approach

- Digital Forensics Technology
- Digital Forensic Tools
- Role of Operating System in Digital Forensics investigation
- Imaging Methods and Storage Technology
- Evidence collection
- Digital Forensics Analysis and Validation
- Recovering Graphics Files
- Evidence Dynamics and Evidence Preservation
- Network Forensics
- E-mail Investigations
- Cyber Crime
- Laws governing Evidence
- Privacy and Ethical aspects of Digital Forensics

These fifteen topics are particularly suitable for a 15-week semester course. The primary thrust of our course was in preparing the students to understand the legal requirements for gathering, preserving, and presenting evidence. As part of this goal we needed to expose the students to some of the hardware aspects, which many seemed to lack because of the heavy emphasis in our program on software. After an initial introduction to the hardware aspects, we looked at simple tools available widely for analyzing network communication.

Much of the course is devoted to understanding the legal requirements related to gathering and analyzing the evidence, having a chain of custody for the evidence, generating the necessary reports based on the evidence, and presenting the evidence in a court. In this connection we reviewed several court cases as to how they dealt with the evidence. Some of the important cases used in the review were NY vs. Ferber, U.S. vs. Frye, U.S. vs. Katz, U.S. vs. Kyllo, U.S. vs. Thomas (Legal, 2010). In this connection we also covered several federal laws concerning protection of children and privacy issues. These laws include the following:

- Sexual Exploitation of Children Act
- Child Protection Act
- Child Sexual Abuse and Pornography Act
- Child Protection and Obscenity Enforcement Act
- Child Pornography Prevention Act
- Child Online Protection Act
- Digital Millennium Copyright Act
- Family Education Rights and Privacy Act
- Electronic Communications Privacy Act
- USA PATRIOT Act of 2001

We devoted several class periods to discuss how cyber crime is committed and how network forensic techniques could be used to track criminals. In order for students to understand the practical aspects of digital forensics, we were able to visit one of FBI's Regional Computer Forensics Labs (RCFL). On another occasion, we had a practicing attorney dealing with digital forensics cases present a talk about the legal aspects of evidence. On several occasions we brought up ethical issues that crop up in investigation and reviewed some ethics related cases. Another important topic that we covered in this course related to emails. This topic particularly attracted students' attention because of their extensive use of a variety of providers for email service. We covered this material from an investigative aspect, using commercial tools such as FTK and Paraben Software. One important part of this discussion was in evaluating the amount of information hidden in email headers for investigative purposes.

Growth of storage technology has led to many small devices such as thumb drives and digital flash cards used in cameras holding large volumes of data. Further, improvements in storage technology such as SATA II have facilitated rapid data transfer between devices. Wireless communication has further facilitated storing data in remote locations using NAS and SAN technologies. From an investigative standpoint these are all challenges to be faced because these types of storage devices are not easy to locate. Moreover, tools such as Host Protected Area (HPA) enable the partitioning of hard disks into hidden areas that are not accessed by the operating system (Gupta, Hoeschele, & Rogers, 2006). We concluded the course with a study of how small electronic devices such as cell phones and PDAs are used extensively to communicate and how much information is stored in various log files relating to these small devices. Extracting such information requires a variety of specialized tools because there is no single standard used by the hardware manufacturers of these small devices. It is expensive to build the tool set to analyze all such devices. Overall, the course material coverage gave the students a sampling of technologies in use that could be abused by computer criminals and how specialized hardware and software tools could be used to extract such evidence directly from such devices as well as from other communication providers such as ISPs.

Laboratory

In order to give the students a strong foundation in digital forensics concepts and practices it is essential to have an opportunity to do hands-on practice. For this purpose a dedicated lab would help. At the least, the students should have the space and computers to open up and identify the inner hardware on a computer. It is our experience that getting used computers was not difficult but having the space to use as a lab might be the problem. Instructors planning a digital forensics course may have to focus on this to see if this resource could be made available.

We were able to find several spare computers and provided the students desk space to open the hardware to see the internals. One assignment involved changing the boot password by removing the battery powering the CMOS chip. These computers were also used to practice "bag and tag" of evidence. For three assignments, we used FTK software. We acquired six hard disks from external sources and supplemented them with a few more hard disks. Each hard disk was assigned to two students. A demonstration version of FTK is available for free from Access Data for teaching purposes. This software covers most essential aspects of a forensics investigation. Each student used the allotted hard disk to run the FTK software to find hidden and deleted files. Students also created host protected areas on their hard disk to hide files. Each student had to find the hidden and deleted files in other students' hard disks.

One of the major tasks of a computer forensic investigator is to find deleted files and files that have been altered to look like they are unusable. In this context it is important to note that there are certain powerful tools such as Evidence Eliminator (2013) which scuttle this aspect of an investigator’s work. When Evidence Eliminator is used to delete a file, then it leaves no trace of that file. The students were given an exercise to test this using both FTK and Evidence Eliminator.

Most criminals, especially people dealing with child pornography, tend to hide files in multiple ways. Some of these approaches may be as simple as changing the file type so that it does not draw the attention of the examiner or so that it will not be identified by the operating system as a file of a particular type. In the next several paragraphs, we will outline other methods of hiding files.

File Hound (2013) is useful free software that does a very good job of finding all image files in a storage device, irrespective of what was done to the file name. The assignment for this involved each student hiding a file in their hard drive and other students discovering such files. Much of

the focus in this course was related to file systems in the form of locating and recovering files, viewing the file contents, checking for hidden storage spaces in hard disks, etc. An excellent resource to learn more about file systems is Carrier's book on File System Forensic Analysis (Carrier, 2005).

A fundamental rule in evidence gathering from a site where law enforcement people converge based on a search warrant is to make a bit-stream image of all storage devices found. A bit-stream image is a copy of all storage content bit-by-bit. This way all hidden and deleted files will be found. In order to make the evidence captured presentable in a court, the bit-stream image should be hashed using MD5 or SHA-1 method and a copy of the bit-stream image along with the hashed values embedded should be left with the owner of the data. A side benefit of bit-stream image is that it lends itself to easy searching for any specific sequence of characters. It is important to note that the hash value does not reveal any information about the original data. Students were given an assignment to demonstrate their grasp of this important aspect of evidence gathering. This is usually time consuming because large volumes of data may have to be copied.

One of the important things to follow with any captured evidence is chain of custody. This means that there should be complete documentation of every activity that was performed with the captured data. This trail should account for the entire period the data was under the control of the person gathering the evidence. Finally, after examining the captured data the examiner must prepare a detailed report indicating the conclusions that could be arrived at from the data. This report would form the basis for any expert testimony in a court.

So far we discussed a conventional laboratory environment. Bem and Huebner (2007) described a scenario where some of the forensic analyses could be done in a virtual environment. Their conclusion was that the virtual environment enables the investigator to gain greater experience in increments than a conventional one. This is another option instructors could consider in examining evidence.

Lessons Learned

In planning for this new course, we lacked the necessary laboratory resources needed for testing. By offering the one-credit course "A+ for Forensics" we were able to identify both the hardware and software requirements from a tools perspective. This led us to acquire the FTK package and the Read/Write blockers necessary to conduct a forensic investigation of a storage device. We were in the same situation as most institutions, where obtaining used hardware was not a major problem but finding financial resources to acquire new software was not easy. This forced us to look for free software tools. We were pleasantly surprised to find many tools with sufficient power to teach the basic forensic concepts. Over the past two years, with the increase in the number of academic offerings, companies such as AccessData have made available some free versions of their popular software (FTK, 2013). We have identified such resources in this paper.

Resources

The main aim of this section is to assist faculty planning to incorporate Digital Forensics as a course in their curriculum by identifying what types of resources are available, what they would cost, and how to obtain them. For this course, we acquired some free software tools as well as some commercial grade tools. We briefly describe each resource that could be obtained for free or for a minimal cost.

Hex editors enable the user to see both the bit values and ASCII values in one screen, line by line. There are several free hex editors available. Tiny Hex Editor is the one we used in our course (Hex Editor, 2013). Taft (2013) is a free tool that interfaces with ATA drives and retrieves a variety of information about the hard disk. It is also used to change the maximum addressable area,

thus creating a HPA to hide data. Timestomp (2013) is a free tool used to modify the NTFS generated data about file creation, access, and modification timestamp values. Evidence Eliminator (2013) is a very powerful tool that completely eliminates all traces of a file. This works counter to what a forensic examiner would want; however, it is essential for the students to know such tools exist as well. This is inexpensive but not free software. File Hound (2013) is available free from CERIAS institute at Purdue University. This software will find all image files, irrespective of their type (JPEG, GIF, TIFF, PNG, etc) and whether the file header was modified or not. Sleuth Kit (2013) is free software that comes with the Autopsy Browser. Both are open source digital forensic tools that run on Windows and UNIX systems. They enable the user to examine a variety of file systems for evidence.

The three popular commercial tool sets are: FTK (Forensic Tool Kit) by Access Data, Encase by Guidance Software, and FRED (Forensic Recovery of Evidence Device) by Digital Intelligence. FTK is an affordable tool for academic institutions. FTK Imager is available for free, which will do many of the functions of the full version. In order to use the software tool, first a write-blocker kit is needed. The full kit (sturdy bright yellow box) costs around $600 but one could acquire just one write-blocker and the cables only from Access Data (FTK, 2013). A free version of FTK demo software is available from AccessData Corp. Encase is a powerful tool and costs significantly more. However, recently Encase (2013) has started offering academic institutions at a more reasonable rate. Interested instructors could contact Guidance Software directly for the details. All the functionalities that Encase offers for the teaching environment also are available from FTK. FRED (2013) is a hardware system with embedded forensic software. It is more expensive than FTK and Encase, but it has many useful features for forensic investigation of hard disks.

One of the main things done first in forensic investigations is in making a true image of the hard disk and other storage devices under investigation for the necessary evidence. All three commercial software mentioned above do this very effectively. However, there is a command in both Windows and Linux/Unix environments called **dd**. This free tool will also facilitate making a true image of a storage device. In preparing the material to cover these topics, several books were used. The publication details for these books are in the References section (Brown, 2009; Kruse & Heiser, 2001; Philipp, Cowen, & Davis, 2009; Phillips, Nelson, Enfinger, & Steuart, 2008; Shinder, 2008; Vacca, 2013).

In addition to these tools, we also examined many network communication tools. This category includes tools such as Nessus, Snort, and Wireshark. All these tools are free.

The tools identified above are widely used in forensic investigations and so they all have practical relevance. The Hex Editor and Taft are useful in gathering information about the storage aspects used to hide information. Timestomp plays a critical role in providing corroborating evidence in a legal setting. Evidence Eliminator's power is to illustrate how a criminal could eliminate evidence. File Hound is useful in detecting images that are hidden by altered file types that would be detected by the file system. Sleuth Kit's use comes in the form of providing evidence to back up a forensic investigation. Newer tools are constantly emerging as newer evasive techniques are developed by the criminal minds to hide evidence of crime. In this effort the work of NIST, in collaboration with the Law Enforcement Standards Office, to develop methodology for testing computer forensic software tools is significant. This resource is important for a forensic examiner to have confidence in the integrity of the software tool used for forensic analysis (NIST, 2013).

Future Enhancements

We have noted the wide popularity of small devices such as high capacity storage devices, powerful cell phones and the ability to access the Internet from mobile devices such as iPhones, iPads

and other Smart phones. Also, the capacity of USB flash drives and digital camera flash cards exceed 16 gigabytes. Consequently, very large amounts of images could be stored in portable devices and hidden. It may be hard to locate these portable devices during an investigation but an analysis of the computer system would at least show the copying of large volumes of data to USB and fire wire based devices. This shows that a significant amount of evidence in investigations might be stored in small appliances. For this reason we plan to enhance our Digital Forensics Laboratory with the capability to examine and gather evidence from such small appliances.

Conclusion

Digital Forensics is an important area of study for information security students because, while computer forensic investigation does not prevent the crime from occurring in the first place, it serves as a powerful deterrent for the criminals to know that their acts can be discovered and prosecuted. Today, we find that financial fraud and child pornography are the two leading areas that are consuming much of the investigators' time. This problem is worldwide and, in addition to the social costs, involves several billion dollars in loss each year to legitimate businesses. The material we have presented above sheds much light into how these things could happen and how an alert person potentially could discover and track any crime committed.

The curriculum details presented in this paper could be of help for any instructor in developing a Digital Forensics course. Anyone planning to develop such a course should have good programming experience and understand simple hardware aspects in order to troubleshoot. A basic knowledge of how client/server systems operate would help in explaining network-based discovery issues. The person interested in creating such a new course would benefit if they start the preparation for the course content in spring semester in order to offer the course in the following fall semester. The main reason for this suggestion is that during the spring semester the instructor will be able to identify the hardware resources that could be gathered and there will be sufficient time to experiment over summer when laboratory demands will be less. From the student perspective, the course would be most interesting and effective if taken after they had courses in networking and database design and had significant programming experience. Typically students in the second semester of junior year would have the necessary background for succeeding in this course. This course would be an excellent addition to the Information Security curriculum. Students in Accounting and Criminal Justice programs would find this course very useful, as well. For accounting students the benefit comes from knowing how technology could be used to hide information so that they could be prepared to unearth hidden data in their audit. Students in Criminal Justice program would benefit by knowing how to handle evidence, the importance of Chain of Custody with computers and media, and what tools are available for the investigator to use to gather and reserve the necessary evidence.

References

Anderson, P., Dornseil, M., Freiling, F. C., Holz, T., Irons, A., Laing, C., & Mink, M.. (2005). *A comparative study of teaching forensics at a university degree level*. Retrieved May 5, 2013 from http://pi1.informatik.uni-mannheim.de/filepool/publications/a-comparative-study-of-teaching-forensics-at-a-university-degree-level.pdf

Austin, R. (2007). Digital forensics on the cheap: Teaching forensics using open source tools. *Information Security Curriculum Development Conference*, Kennesaw, GA, Article 6, 1-5. http://science.kennesaw.edu/~rausti19/ISA4350Files/ForensicsCheapProceedings.pdf

Batten, L., & Pan, L. (2008). Teaching digital forensics to undergraduate students. *IEEE Security and Privacy, 6*, 54-56.

Bem, D., & Huebner, E. (2007). Computer forensic analysis in a virtual environment. *International Journal of Digital Evidence*, *6*(2), 1-13. Retrieved from http://xa.yimg.com/kq/groups/19242253/187320131/name/CCP-+Computer+Forensic+Analysis+in+a+Virtual

Brown, C. L. T. (2009). *Computer evidence: Collection and preservation* (2nd ed.). Boston, MA: Charles River Media.

Carrier, B. (2005). *File system forensic analysis.* Boston, MA: Addison-Wesley.

Chi, H. (2009). *Design and implementation of digital forensics labs: A case study for teaching digital forensics to undergraduate students*. Retrieved May 5, 2013 from http://www.famu.edu/cis/year2009-Chi-Jones-etal-CATE.pdf

Encase. (2013). Retrieved May 5, 2013 from http://guidancessoftware.com

Evidence Eliminator. (2013). Retrieved May 5, 2013 from http://www.evidence-eliminator.com

File Hound. (2013). Retrieved May 5, 2013 from http://filehound.cerias.purdue.edu/get.html

FRED. (2013). Retrieved May 5, 2013 from http://www.digitalintelligence.com

FTK. (2013). Retrieved May 5, 2013 from http://www.accessdata.com

G8 Summit. (2000). Retrieved May 5, 2013 from www.ioce.org/fileadmin/user_upload/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf

Gupta, M., Hoeschele, M., & Rogers, M. (2006). Hidden disk areas: HPA and DCO. *International Journal of Digital Evidence*, *5*(1), 1-8. http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf

Hex Editor. (2013). Retrieved May 5, 2013 from http://www.softpedia.com/get/Programming/File-Editors/Tiny-Hex-Editor.shtml

Kruse, W., & Heiser, J. (2001). *Computer forensics: Incident response essentials.* Boston, MA: Addison-Wesley.

Legal. (2010).

Ferber-1982. Retrieved May 5, 2013 from http://www.law.cornell.edu/supct/html/historics/USSC_CR_0458_0747_ZS.html

Frye-1992: Retrieved May 5, 2013 from http://www.law.ufl.edu/faculty/little/topic8.pdf

Katz-1967: Retrieved May 5, 2013 from http://www.oyez.org/cases/1960-1969/1967/1967_35/

Kyllo-2001: Retrieved May 5, 2013 from http://www.law.cornell.edu/supct/html/99-8508.ZS.html

Thomas-1996: Retrieved May 5, 2013 from http://www.tomwbell.com/NetLaw/Ch04/Thomas.html

Lim, N. (2006). Crime investigation: A course in computer forensics. *Communications of AIS*, *18*(10), Article 10.

Lunn, D. (2001). *Computer forensics – An overview.* SANS Institute. Retrieved from http://www.giac.org/paper/gsec/559/computer-forensics-overview/101340

NIST. (2013). Retrieved May 5, 2013 from http://www.nist.gov/oles/forensics/digital_evidence.cfm

Noblett, M., Pollitt, M., & Presley, L. (2000). Recovering and examining computer forensic evidence. *Forensic Science Communications, 2*(4). Retrieved from http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

Philipp, A., Cowen, D., & Davis, C. (2009). *Computer forensics – Hacking exposed: Secrets and solutions* (2nd ed.). New York, NY: Osborne-McGraw Hill.

Phillips, A., Nelson, B., Enfinger, F., & Steuart, C. (2008). *Guide to computer forensics and investigations* (3rd ed.). Boston, MA: Course Technology.

RCFL. (2013). *FBI Regional Computer Forensics Laboratories*. Retrieved May 5, 2013 from http://www.rcfl.gov

Shinder, D., & Cross, M. (2008). *Scene of the cybercrime* (2nd ed.). Waltham, MA: Syngress Publishing.

Sleuth Kit. (2013). Retrieved May 5, 2013 from http://www.sleuthkit.org/sleuthkit

Stander, A., & Johnston, K. (2007). The need for and contents of a course in forensic information systems & computer science at the University of Cape Town. *Issues in Informing Science and Information Technology*, *4*, 63-72.

Standler, R. (1998). *Privacy of email in the USA*. Retrieved May 5, 2013 from http://www.rbs2.com/email.htm

Taft. (2013). Retrieved May 5, 2013 from http://vidstrom.net/stools/taft

Timestomp. (2013). Retrieved May 5, 2013 from http://www.anti-forensics.com/tag/timestompexe

Vacca, J. (2013). *Computer forensics: Computer crime scene investigation* (3rd ed.). Burlington, MA: Jones & Bartlett Publishers.

Whitcomb, C. (2002). An historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, *1*(1). Retrieved from http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

Yasinsac, A., & Manzano, Y. (2001). Policies to enhance computer and network forensics. *Proceedings of IEEE Workshop on Information Assurance and Security, Westpoint, NY, June.* http://www.cs.fsu.edu/~yasinsac/Papers/MY01.pdf

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P.M. (2003). Computer forensics education. *IEEE Computer Security and Privacy Magazine*, *1*(4), 15-23.

Biography

Srinivasan is Professor and Chairman of International Business and Technology Studies at Texas A and M International University. Prior to joining TAMIU he was at the University of Louisville from 1987 to 2010. He started the Information Assurance program at U of L in 2003. This program was designated a National Center of Academic Excellence in IA Education by NSA/DHS. His research interests are in Information Security. He has published several papers in both Mathematics and Computer Science. Currently he concentrates his teaching and research in Information Security related topics involving Social Media, Cloud Computing, RFID and SCADA. He is currently working on two books on Cloud Computing to be published in 2013. He is the recipient of several grants for security related projects. He spent his sabbatical years at GE, UPS and Siemens. He volunteers his time extensively for public education causes.