Implementing a Digital Forensics Lab in Education

Steve Scott

Abstract— Cybercrime is and has been on the rise for several decades and a rise in this specific criminal activity is only expected to continue. This increase in cybercrime activity results in a need for specially trained investigators. Individuals specially trained to retrieve information from computers or other digital devices are known as digital forensics investigators. These types of investigators require training that is somewhat more comprehensive than that of the typical information technology student. Training a digital forensics investigator requires hands on experience with actual equipment in addition to traditional training methods of theory and testing. Hands on training can be accomplished through the construction and management of a student lab built specifically for digital forensic investigative training. There are many things to consider when constructing a lab. Two of the largest expenses when outfitting a student lab are the software and hardware to be used. The type of investigative software to be used is typically the first consideration as the software's system hardware requirements will be the driver for the type of workstation that will be used. A lab can be outfitted with varying different software solutions that range from commercial investigative suites to free command line tools. In much the same way, the forensic workstations that will be running the software can be vendor supplied standalone units or can be built with individual components in house. Both of these decisions are most likely driven by monetary constraints in an educational setting. There are also a multitude of other particulars that must be considered such as lab location, peripherals and network topography as well as others. The successful construction and management of a student lab can be a daunting endeavor but can be accomplished even with a small budget so long as focus remains on student success.

Index Terms—Cybercrime, Digital Forensics, Student Lab, Education

1 Introduction

With advances in technology as well as increased global Internet access and simplification of tools used to commit crimes using technology, occurrences of cybercrime activity have been on a steady increase over the last decade. Cybercrime is defined as crimes committed on the Internet using the computer as either a tool or a targeted victim [1]. Interpol divides cybercrime into three broad areas [2]:

- Attacks against computer hardware and software – malware, network intrusions, denial of service attacks
- Financial crimes and corruption – fraud, phishing schemes
- Abuse – sexploitation, crimes against children, harassment

In the past, cybercrimes were primarily committed by individuals but modern day cybercriminal activity is often committed by highly organized, technologically savvy criminal organizations and even State Governments. Generally speaking, the crimes are not new; what is new is the ease at which crimes can be committed due to the rapid expanse and availability of the Internet to both criminals and their victims. According to the United States Department of Justice, cybercrime has become one of the greatest threats facing our country and has enormous implications for our national security, economic prosperity, and public safety [3]. In 2014, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center received 269,422 complaints regarding Internet crimes and logged its three millionth complaint since its 2001 inception. [4]. This relatively new type of crime brings the necessity for a new type of investigative science known as computer or digital forensics. The word forensics comes from the Latin word foresis which means to "bring to court" and involves the reclamation and analysis of evidence for presentation to a court. Much like any other forensic evidence such as fingerprints or hair samples, evidentiary data exists on computing devices that can be admissible as evidence in a criminal or civil case. The goal of digital forensics is to identify, collect, preserve, analyze and present this data in such a way that it can be used as evidence in a court proceeding. To accomplish this requires an investigator that specializes in the recovery of data from computers as well as other types of electronic devices. Digital forensics investigators not only perform data analysis and recovery but are often called upon to serve as expert witnesses during the actual court proceeding that they may be investigating. This requires a very thorough understanding of current as well as past technologies. The role of the digital forensics investigator is unique in the world of information technology (IT) specialists because of the inherent necessity for such a broad range of specific technological knowledge. Many IT fields today are compartmentalized in a way that allows an IT technician to be very effective in their particular area of expertise but at the cost of little or no knowledge of IT as

a whole or other specific technical aspects of a technology. A digital forensics investigator is required to possess specific technical knowledge of an operating system from how the file system writes data and how to use the GUI to how the system communicates across a network. Attention to detail and thoroughness are both essential to fulfill the role. Much of an investigator's time is spent writing reports on their findings and in preparation to present and defend findings in court. The field of information security has a much faster than average job outlook for the next several years according to the US Department of Labor. The US Bureau of Labor Statistics job outlook for Information Security Analysts, which digital forensic investigators are a subset of, is predicted to have a 37% increase from the time period 2012-2022 with a median pay of $86,170 [5]. Such a skill set requires targeted training not only to keep up with projected demands but to keep the investigator on par or a step ahead of the perpetrators of cybercrimes. Increased need for training is necessitated by the inherent continual changes to the IT field as a whole. The IT field is constantly experiencing changes ranging from the way in which data is physically stored to entire platform changes on a global scale.

2 Institutional Response

Educational institutions have responded to the need for trained investigators by implementing various degree and certificate programs in digital forensics. Training a student in digital forensics, or any investigative field, has unique challenges in that educators are tasked with teaching a student how to process through a case and find evidence through discovery without an absolute definitive template on how to do so. Every case is different every time and there can be no "cookbook" or paint by the numbers method for investigative processes. The investigative process of a digital forensics examination cannot be accomplished by following a set of steps on a reference card. Accomplishing an effective curriculum requires activities beyond theoretical lectures and multiple choice quizzes. A digital forensics curriculum must consist of hands-on lab work that is completed by students performing exercises and examinations on real equipment in a lab environment. Theory is better understood when it can be practiced or applied [6]. This method of teaching facilitates kinesthetic learning in which students learn by performing physical activities in lieu of listening to lectures or reading PowerPoints. Kinesthetic learning takes place and students learn more when they are actively engaged in learning via hands-on practice and other means [7]. The challenge to students gaining practical knowledge by the way of hands-on experience lies in building and maintaining a suitable lab environment for training. Building and maintaining such a lab can be a daunting undertaking due to the many considerations that must be made to include room requirements, software, hardware, network concerns and many other miscellaneous peripherals and devices that are needed for such a program.

3 Physical Requirments

The physical space that a digital forensics lab occupies must be able to effectively facilitate student learning. To accomplish this, the student lab should be created in a way that is as close as possible to an actual functioning crime lab. The room must be large enough to accommodate a number of forensics workstations as well as ample work areas around each station. In addition to the individual workstations, space will be required for a network license server. Typically a network license server is required to provide a centralized distribution point for forensic software licensing. This is a requirement for most examination software suits that have very stringent security requirements for their licensure. It should include shelving and/or cabinets to house peripherals as well as printed material such as documentary evidence and product manuals. The space would also require enough room for workbenches to perform examinations on devices that are not traditionally done with using a forensic workstation such as separate hardware imagers and many phone examination tools. A high security storage device such as a safe or cabinet must be used to store original evidentiary items and working copies that contain sensitive information. The storage devices used to store evidence should be environmentally secure and able to withstand fire or flood damage. The entire room should be secured from general access, ideally with a cypher or pass card locking system to audit room entries and control admittance. The workstation monitors and equipment should not be in view of the general public due to the nature of sensitive information that is examined in a forensics examination. This is not an absolute requirement in a training environment because actual contraband such as child pornography or other sensitive information is not actually used. Contraband is mimicked in a training environment to provide a realistic discovery process for the student. Finally, the room should provide ample power and cooling as well as be free from dust, electronic hazards or debris. Power and cooling are especially important in a digital forensics lab as opposed to a typical computer lab that a student may use. During case processing, it is common for the workstations that are processing evidentiary data to utilize one hundred percent of their resources for extended periods of time, for days or even weeks straight. A forensic lab that houses eight or more workstations in a small space heats up very quickly without adequate cooling potentially causing damage to equipment as well as evidence that is being processed. The workstations also use significantly more power when processing requiring the possibility of additional power considerations. The necessity for room organization and cleanliness cannot be

overstated. Many times, the evidentiary value of computers in traditional evidence rooms has been inadvertently destroyed by carelessness, dust, or unhealthy climate conditions [8]. Most physical space requirements will be based on the number of workstations that the lab will house according to how many students will be trained. Typically, both of these decisions are ultimately decided on the budget for the project. Another item for consideration that must take place before workstation hardware is decided upon is the examination software.

4 SOFTWARE

Digital forensic examination software is available from full commercial software suites all the way down to command line freeware batch files to parse information. One of the first things that must be considered is what operating system will the lab workstations use. Most of the high end commercial software only runs on Microsoft Windows while many of the free forensics software tools only run on the Linux operating system. An ideal instructional environment uses both to expose students not only to different examination tools but also to the intricacies of the differing operating system platforms.

The most popular commercial examination software suites today are Forensic Toolkit (FTK) by AccessData and EnCase by Guidance Software. Both commercial offerings are used by law enforcement, have their strengths and weaknesses and are often compared and contrasted to one another. AccessData describes FTK as a court-cited digital investigations platform built for speed, stability and ease of use. It provides comprehensive processing and indexing up front, so filtering and searching is faster than with any other product [9]. FTK is well known for the use of up front indexing that provides for nearly instantaneous search results. The examination suite also includes a standalone imager, registry viewer and password recovery tool. EnCase is described by Guidance Software as the global standard in digital investigation technology for forensic practitioners who need to conduct efficient, forensically-sound data collection and investigations using a repeatable and defensible process [10]. It too contains additional tools such as a standalone imager and decryption solutions in the form of modules. Both suites are also well known for their distributed processing capability in which the software can use up to eight workstations to process a case simultaneously. This speeds up case processing exponentially, reducing case process times from days to hours. Although these commercial applications can be quite expensive, they both have academic programs that reduce the cost significantly for educational use. Both have extensive training programs that can be utilized to "train the trainers" of a newly created program. Some of the cost of commercial software can be offset by these benefits. Another benefit of the commercial suites such as FTK and EnCase is that they both offer industry recognized certifications on the use and proficiency of their products. FTK issues the AccessData Certified Examiner (ACE) credential and EnCase has a similar certification, EnCase Certified Examiner (EnCE). Both of these credentials can be obtained by students upon completion of a program and can aid them in their employment searches.

There are many, many free digital forensics investigative tools. Most run only on Linux and many are command line only without a graphical user interface (GUI). Some of the more well-known and often used free tools include SANS SIFT, Sleuth Kit, Caine, Oxygen and Paladin. Sleuth Kit is a collection of command line Linux tools for data analysis and recovery. It has a GUI based Windows counterpart named Autopsy that uses modular plug-ins much like EnCase. The other free tools listed above are all Linux boot disks that allow a user to run an instance of Linux in a protected environment in which to perform a forensic examination. They are each a suite of sorts that contain a variety of tools for imaging and data analysis. Most of the Linux boot disk solutions above are best utilized as triage or incident response tools when full case processing is not pertinent typically due to time constraints. These tools are portable and can be up and running in a very short time. They are often used on scene to extract or examine information on the fly when time is of the essence. That is not to say that they are any less effective than the commercial suites; the commercial tools are typically easier to use for an entry level student. Both types of tools examine data equally and an entire digital forensics program could, and has been, built around free tool sets. Examination software considerations are particularly important as they are the driver for hardware needs. All of the software will have a set of minimum and recommended hardware requirements. The recommended/required specifications must be carefully considered when specifying hardware that will be used in the student lab. Hence the choice of software used in the digital forensics program can be a large part of determining hardware needs and ultimately cost.

5 HARDWARE

Digital forensics workstations can be purchased as complete, turnkey special purpose units from vendors or custom built from individual parts. Special purpose units such as the Forensic Recovery of Evidence Device (FRED) from Digital Intelligence, Talino from Sumuri or the Velocity series from Tritech Forensics are available in many configurations and range in price from around three thousand all the way up to sixteen thousand dollars and above. These turnkey solutions have both advantages and disadvantages when building a forensics lab for student use. They are all complete units that arrive with an operating system as well as many differing input/output (I/O) connections to accommodate various types of media that are encountered in the field. They will come with a manufacturer's warranty, monitors and are the type of workstation that an examiner will be exposed to in most, if not

all, modern working labs. Using a purpose built workstation exposes the student to the type of device they are most likely to encounter in the real working world. The obvious disadvantage is of course cost. The standard configuration FRED system costs $5999.00 [11]; outfitting an eight workstation lab with just this baseline device will cost around $48,000.00. This is very cost prohibitive to most educational institutions that will likely choose to build their own systems using individual parts. Building custom systems with parts is a much more affordable solution and can be configured to meet the chosen software needs as well as institutional needs. In addition; a custom built workstation also allows for future hardware upgrades as needed due to the modularity of a custom built unit. Building out a lab with custom built workstations allows a program to be started that is on a smaller budget that can be upgraded incrementally as more funds become available. Purchasing the turnkey units requires a large, upfront cost that may not be possible for every institution. There is also educational value not only for the students, but also for the program staff in researching software requirements, sourcing the required parts and finally assembling a complete unit and subsequently an entire lab. An assignment lab for students can in fact be the process of researching hardware requirements and the actual assembling of lab computers to act as forensic workstations. Making the decision to outfit a student lab with custom built workstations allows for the construction of a purpose built network license server for the examination software licensure. The network server will not require the high specifications of the examination workstations and can be a basic system with network access. It would be facetious to outline a parts and price guide for building custom systems as component capabilities and prices literally change on a daily basis. Suffice to say that custom built systems should be built with the latest, fastest and highest quality components that are within the budgetary constraints of the program. One of the largest challenges in computer crime is coping with huge amounts of data [12]. As data amounts increase there is an increased need for faster and faster I/O functionality of the examinations stations making I/O speed the number one point of focus when allocating limited funds. Particular emphasis should be placed on outfitting the machines with the fastest I/O components possible such as solid state hard drives (SSDs), system buses, and a multitude of I/O interfaces to accommodate the varying types of media to be examined. Monitors, keyboards and mice must be provided to complete a custom workstation buildout. Dual monitors are ideal due to the very large amount of information that is displayed by the examination software. If dual monitors are not feasible, single large widescreen monitors should be used. Forensic workstations will make up the majority of a labs expenditures and equipment but they are not the only devices that must be considered when outfitting a student lab.

6 Peripherals

In addition to the examination workstations and network server, the lab will require a certain amount of miscellaneous peripherals that are required in the examination process. These items include:

- Hardware write blockers
- Hard disk drives
- Various cables and adaptors
- Anti-static mats
- Computer tool kits

Hardware write blockers are devices that allow the creation of a forensically sound image file of a suspect computer or hard drive. They work by allowing only read commands across a data link and block any write commands from occurring. This procedure is crucial in forensic image creation as it is imperative that data is not written to the suspect drive under examination. Sound image creation is of utmost importance in the forensic examination process as the golden rule of electronic evidence is never modify the original media [13]. Just like any other physical evidence, if the suspect data is modified or tainted it can become inadmissible in court placing the entire case at risk. Hardware write blockers allow the passage of data from a suspect drive to a working evidence drive. The lab must also be equipped with varying types of hard disk drives to accommodate the working evidence image creation process. Drives should be of varying sizes and interfaces to expose students to the many different types of data storage that they may encounter. Hard drive interface types should include:

- IDE
- SATA
- SCSI
- Fiber Channel

The lab should be equipped with cables and adaptors to accommodate the different hard drive types as well as other external data sources such as:

- USB
- Firewire (IEEE 1394)
- Thunderbolt
- eSATA
- Serial
- Parallel
- RJ-45
- BNC
- mSATA
- SATA Express

A final consideration on lab equipment should include an emphasis on mobile investigation tools such as the standalone Cellbrite UFED or any number of commercial or open source mobile specific investigation tools such as Lantern or Accessdata's Mobile Phone Examiner (MPE). 90% of American adults have a cell phone and 58% have a smartphone. This represents a 37% increase in cell phone ownership since the year 2000 [14]. Many investigative agencies, both local and Federal, have shifted from a focus on desktop examinations to mobile examinations [13]. This makes proficiency with mobile investigations of the utmost importance to future digital forensic examiners and should be a primary consideration when constructing a student lab.

7 Conclusion

Increases in cybercrime activity demand the need for properly trained investigators and that need is expected to continually increase. Institutions in higher education can respond by offering education and training in the digital forensics field of study. To do so requires a capital investment to provide a hands on learning environment in which students can use the actual hardware and software that is used in the working world of digital forensics. A student lab can fulfill the need for hands on experience and provide a foundation for continual training. This paper has presented a broad overview of a generalized student lab setup. The specific lab workstations and software can be of varying types and costs depending on the institution's budget. Emphasis should continually be placed on emerging technologies to better prepare students for investigative careers. The primary emphasis in any program should of course always focus on student learning and this can be more effectively accomplished through the construction and use of a purpose built digital forensics student lab.

References

[1] A. E. Joseph, "Cybercrime Definition," 28 June 2006. [Online]. Available: http://www.crime-research.org/articles/joseph06/.

[2] Interpol, "Cybercrime/Cybercrime Areas," 2015. [Online]. Available: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[3] US Department of Justice, "Cyber Crime," 23 December 2014. [Online]. Available: http://www.justice.gov/usao/priority-areas/cyber-crime.

[4] Federal Bureau of Investigation, "2014 Internet Crime Report," 2015. [Online]. Available: http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf.

[5] United States Department of Labor, "Information Security Analysts: Occupational Outlook Handbook," 8 January 2014. [Online]. Available: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[6] K. Floyd and J. Yerby, "Development of a Digital Forensics Lab to Support Active Learning," in SAIS 2014 Proceedings, 2014.

[7] M. Taylor, "Teaching Generation NeXt: A Pedagogy for Today's Learners," A Collection of Papers on Self-Study and Institutional Improvment, 26, pp. 192-196, 2010.

[8] M. Britz, Computer Forensics and Cyber Crime: An Introduction, Upper Saddle River: Peason Education, 2013.

[9] AccessData, Inc., "Forensic Toolkit (FTK)," 2015. [Online]. Available: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk.

[10] Guidance Software, "Computer Forensics Software - Encase Forensic," 2015. [Online]. Available: https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx.

[11] Digital Intelligence, "FRED," 2015. [Online]. Available: http://www.digitalintelligence.com/products/fred/.

[12] Frank Breitinger, "Towards a Process Model for Hash Functions in Digital Forensics," in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Moscow, 2014.

[13] M. Rogers, Interviewee, Digital Forensics Investigator - Hickory Police Department. [Interview]. 7 June 2015.

[14] M. Arnold and D. R. Kiker, "The Big Data Collection Problem of Little Mobile Devices," Richmond Journal of Law & Technology 21.3, p. 3, 2015.