BUILDING A DIGITAL FORENSIC LABORATORY FOR AN EDUCATIONAL INSTITUTE

Mousa Al Falayleh
College of Computer Information Technology
American University in the Emirates (AUE)
Dubai, United Arab Emirates
mousa.falayleh@aue.ae

ABSTRACT
The fast growing rates of cyber crimes in recent years has raised the need for qualified digital crime investigators to be on high demand. At the present, various educational institutions start to offer Digital Forensics and Cyber Security as separate degree or specialization at both undergraduate and postgraduate levels. Education in information security in general is based on theoretical principles and analysis together with vast amount of experiments and laboratory work. This paper is proposed to help educational institutes to build an appropriate Digital Forensics Lab that facilitate training for its students and certification for the local community.

KEYWORDS

1 INTRODUCTION
In 2011, the Internet Crime Complaint Center (IC3) actively address crimes committed using the Internet, providing services to both victims of online crimes and to law enforcement. IC3’s report revealed some statistics stating that IC3 received over 300,000 complaints, a 3.4% increase over the previous year[1]. The adjusted dollar loss of complaints was $485.3 million.

Moreover, The Federal Bureau of Investigation’s (FBI) Regional Computer Forensics Laboratory (RCFL) Program revealed Program’s accomplishments in fiscal year 2011 (FY11) [2]. The number of digital forensics examinations conducted by RCFL personnel was 7,629. Additionally, RCFLs collectively processed 4,263 TBs of data in FY11. The fast growing rates of cyber crimes in recent years has raised the need for qualified digital crime investigators to be on high demand.

Cyber Crime (also called computer crime, hi-tech crime, and e-crime) is used to describe criminal activity in which computers or networks are a tool, a target, or a place of criminal activity. A few examples of cyber crime include: Theft of Intellectual Property, Identify Theft, Copyright Piracy, Child Pornography, Illegal Gambling, Planting of Virus and Worms, Storing Illegal Information, Hacking, Password Trafficking, Social Engineering and Fraud.

Digital forensics is a collection of specialized techniques, processes, and procedures used to preserve, extract, analyze, and present electronic evidence that is found in digital devices, often in relation to computer or cyber crime [3]. Digital forensics professionals typically
provide an expert opinion in a court of law or other legal and/or administrative proceeding as to what was found in a suspect electronic device. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

The National Institute of Standards and Technology, NIST, divide digital forensics investigation into four phases [3], which are briefly summarized below:

1. **Collection**: Identify, label, record and acquire data from possible sources, while preserving the integrity of the data.
2. **Examination**: Use manual and automated methods to assess and extract data of particular interest, while preserving the integrity of the data.
3. **Analysis**: Use legally justifiable methods and techniques to derive useful information.
4. **Reporting**: Describe actions used, explain how tools and procedures were selected, determine what other actions need to be performed, including forensic examination of additional data sources, securing identified vulnerabilities and improving existing security controls. Recommend improvements to policies, guidelines, procedures, tools and other aspects of the forensic process.

Digital Forensics is a multidisciplinary field that spans the needs of police and homeland security, law enforcement and the private sector [4]. As well as identifying direct evidence of a crime, digital forensics can be used in the recovery of various sorts of electronic files including deleted, encrypted, and corrupted files. Additionally, it is used in auditing network access, resource usage, and analyzing user activities.

Computer forensics is a growing field of law enforcement, as trained investigators and security officials combine their knowledge of criminal justice and technical expertise to recover vital data, search networks for clues, and solve identity theft emergencies. Some work directly for police departments, while others freelance, or are employed by private detective agencies. If there is a general lack of understanding of digital evidence, this can cause an innocent defendant to be wrongfully convicted [5]. Whatever the case, anyone who wishes to work within the field of computer forensics must first learn the essential skills to succeed. There is a huge demand for digital forensics professionals in the market especially with the wide spread of cyber crimes.

At the present, various educational institutions are responding to market needs and start to offer Digital Forensics and Cyber Security as a separate degree or specialization at both undergraduate and post graduate levels [6]. Education in Digital Forensics is better served by a laboratory work that reinforces principles and theoretical analysis learned in the classroom [7]. Graduates of such program need to be one step ahead thinkers from the criminals in order to fight or investigate crimes. Therefore, they need to be equipped with the required practical knowledge. However, a Digital Forensics lab is difficult to build and maintain, as it needs to be dedicated and isolated, and can not be part of a general purpose.
This paper is proposed to help any new entrance from educational institutions that are aiming to offer Computer Forensics Degree Program, to build their Digital Forensics lab.

This paper is organized as follows. Section 2 explores various usages of a digital forensics lab. Section 3 focuses on the main physical requirement. Section 4 provides some guidance about selecting a digital forensics workstation. Section 5 introduces write blockers while Section 6 lists some miscellaneous items that you have to purchase for your lab. Section 7 explores multi-purposed digital forensic software products while Section 8 provides a review about mobile forensics tools. Section 9 discusses some issues and challenges in the task of building the lab. Finally, Section 10 gives some concluding remarks.

2 DIGITAL FORENSICS LABORATORY USAGES

There are different benefits of having appropriate Digital Forensics lab that facilitate training for an educational institution students and certification for the local community including students and other parties such as local police forces and others.

Digital Forensics students may use the lab in studying the following subjects, just to mention some:
1. Introduction to computer crime studies.
2. Computer crime and investigation techniques.
3. Intrusion forensics.
5. Mobile device forensics

Local community may benefit from the lab in studying the following certification programs in the area of Digital Forensics including [8]:
1. EnCase Certified Examiner (EnCE) Certification
2. AccessData Certified Examiner (ACE) Certification
3. EC-Council Computer Hacking Forensic Investigator (CHFI)
4. CyberSecurity Institute - Computer Forensic Certification
5. International Association of Computer Investigative Specialists (IACIS)
6. Paraben Certified Mobile Examiner (PCME)
7. SANS GIAC Certified Forensics Analyst (GCFA)

3 THE PHYSICAL REQUIREMENTS OF THE LAB

Computer forensics labs come in a variety of setups and arrangements. Most of the investigative process and students work is performed at the lab. Therefore, the lab should provide a safe and secure physical environment oriented to preserve the integrity of the evidence data and the work done there [8]. In what follow, we provide a list of the minimum physical requirements:

a. Mid-size room.
b. Door access with a locking mechanism
c. Evidence container, such as a safe or heavy-duty file cabinet with a quality padlock
d. The lab server
e. A number of digital forensics workstations.
 f. A number of workbenches.
g. Conference table with chairs.
h. Shelves for the lab internal library.
i. Communications options: LAN with limited access to the Internet.

4 DIGITAL FORENSICS WORKSTATION

Digital Forensic Workstation should be selected according to the assigned budget by the host academic institution. Their use also depends on the tasks you have to do. A Forensic Workstation should provide the ability to easily duplicate evidence directly from various storage medias such as IDE/SCSI/SATA hard drives, USB devices, Firewire devices, floppies, CDs, DVDs, LTO-4 tapes and PC Card/Smartmedia/SD-MMC/Memory Stick/Compact Flash media in a forensically sound environment. You have two options in hand: either you buy the special purpose forensics workstations or you build customized ones yourself.

4.1 Special Purpose Forensic Workstation

A special purpose forensic workstation consists of integrated forensic processing platforms that are capable of handling the most challenging computer crime case. The special workstations typically contains a set of removable hard drives that can be used for evidence storage, see Figure 1. The following Write Blocker typically is integrated within the forensic workstation:

- Integrated IDE Drive Write Blocker
- Integrated SATA Drive Write Blocker
- Integrated SCSI Drive Write Blocker
- Integrated USB Write Blocker
- Integrated Firewire IEEE 1394b Write Blocker

“FRED” is an example of special purpose forensic workstation from Digital Intelligence [9], see Figure 1.

Figure 1. “FRED”: an example of the special purpose forensic workstations.

4.2 Basic Customized Forensic Workstation

In case your institution can not afford to buy special purpose forensic workstations as they are expensive, you might go with the customized option. Customized forensic workstations are affordable and can be assembled to suit your institution needs. In what follows, we provide the following specification for such workstation as guidance:

- Mid or full height ATX computer case
- 600 Watt Power supply or better
- Intel i7 (Quad Processor) or find the fastest processor
- 8 GB DDR3 RAM or get as much RAM as your motherboard can support.
- 10/100/1000 Integrated LAN
- 512 MB DDR Video Card (Dual Head) or better
- One external FireWire IEEE 1394a (400 MB/s) Port.
• Two external FireWire IEEE 1394b (800 MB/s) Ports.
• Front mounted USB 3.0/2.0 ports
• eSATA port.
• Dual layer DVD +/-RW drive
• One 300 GB 10,000 RPM SATA hard disk drive (boot/OS drive). The rotation speed for this hard drive is advised to be 10,000 RPM, as this speed delivers a reasonable combination of reliability, acceptable noise levels and performance. If you can not get 10,000 RPM, then 7,200 RPM will do.
• One 2.0 TB 10,000 RPM SATA hard drive (Image storage). It will be used to store course material, practical exercise data, and images that students acquire.
• 22” LCD Monitor

Your customized forensic workstation should have the following OS:
• Microsoft Windows 7 Ultimate 64 Bit With Windows XP Mode
• Microsoft Windows 98SE Standalone DOS
• Linux OS by SUSE or Ubuntu

It is advised as well that your customized forensic workstations have the following licensed Software applications:
• Norton GHOST
• Quicken
• Programming languages
• Specialized viewers [10]
• Microsoft Office.
• Corel Office Suite
• StarOffice/OpenOffice
• Peachtree accounting applications

4.3 Lab Server

You need to supply one computer to be used as a lab server. This computer will be required to have a Gigabit Ethernet card, approximately 2 TB of storage space, an Intel Core 2 Duo or better processor, and at least 8 GB of RAM. It will be used to store software license keys, course material, practical exercise data, and images of the student computers. It should be running one of the following operating systems:
• Windows Server 2003
• Windows Server 2008
• Windows 7

5 WRITE BLOCKERS

Write blockers are devices that allow a forensically sound image of virtually any hard drive or storage device you may encounter without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but by blocking write commands, hence their name.

There are both hardware and software write blockers. Some software write blockers are designed for a specific operating system. One designed for Windows will not work on Linux. It is advised to use hardware write blockers as they are recognized as a court-validated standard. Hardware write blockers are more reliable than software ones. Moreover, hardware write blockers are software independent.

Hardware write blockers/forensic bridges from Tableau are very reliable [11]. You may purchase them directly from Tableau or from some other entities such as The UltraKit III from Digital Intelligence [12], see Figure 2. The
UltraKit III is a portable kit which contains a complete family of hardware write blockers along with adapters and connectors for use in acquiring a forensically sound image. Some other manufacturers of hardware write blockers are:

- WiebeTech
- Logicube
- ICS Drive Lock

Figure 2. Tableau, The UltraKit III hardware write blockers.

6 OTHER MISCELLANEOUS ITEMS

6.1 Stocking Hard Drives

A collection of hard drives will be required for use by students during training and practical exercises. You will need to provide at least 24 hard drives for storage of data during these exercises. 500 GB SATA drives are recommended for this purpose. A collection of 15 smaller capacity (approximately 150 GB) IDE hard drives for imaging training purposes is also advised. A set of 12 external USB-bridged, self powered hard drives of at least 500 GB size for storage of images is also recommended.

6.2 Stocking Hardware Peripherals

You should have the following accessory items in the lab besides workstations and software, including:

1. Power cords
2. Used hard disk drives
3. Computer hand tools
4. Anti-static mats
5. The following drive Interface Cables:
   - One 8" IDE Interface Cable
   - One 2" IDE Interface Cable
   - One SATA Interface Cable
   - One SCSI-3 Interface Cable
   - One 1.8" Hard Drive Adapter
   - One 2.5" Hard Drive Adapter
   - One ZIF Hard Drive Adapter
   - One MicroSATA Adapter

6. Computer Interface Cables/Adapters

- One eSATA to eSATA Cable
- Two USB A to Mini 5 pin Cables
- One FireWire A (6 pin - 6 pin) Cable
- Two FireWire B (9 pin - 9 pin) Cables
- One FireWire A (4 pin - 9 pin) Adapter
- One FireWire A (6 pin - 9 pin) Adapter

7 COMPUTER INVESTIGATIONS AND FORENSICS ANALYSIS SOFTWARE

The following multi-purposed digital forensic software products come from leading developers in this field and cover all aspect of forensic investigation from producing the initial image of the suspect hard disk, through to detailed analysis of emails and internet use:
7.1 EnCase From Guidance Software

EnCase Forensic, by Guidance Software [13], is one of the world's leading solutions for computer investigations and forensics. Together with FTK, They are recognized as court-validated standard in computer forensics software.

EnCase has an academic program that enables Universities to offer every students with hands-on experience. The EnCase Academic Program includes everything a University needs to effectively incorporate EnCase into their curriculum. EnCase Academic Program includes: EnCase Enterprise 12-user academic license, One EnCase Forensic Times NAS security key, and supporting Documentation for both Instructor and student. The security key or dongle is attached to the lab server and then all workstations in the lab obtain the license key from the server.

7.2 FTK From AccessData

Forensic Toolkit (FTK) is a forensic product from AccessData [14]. It enables your lab to expand its forensic capabilities as your needs grow. You may purchase AccessData FTK 12-user academic license. In order to complete the purchase process, you should have somebody among your staff to be qualified as AccessData Certified Examiner (ACE).

The dilemma of whether to buy both EnCase and FTK is needed to be solved. Both products are recognized by courts. Moreover, it is always good to train your students and make them familiar with both tools that are widely used in marketplace. If you are on a tight budget, then we recommend buying the EnCase.

8 SMALL SCALE DIGITAL
DEVICE FORENSIC SOLUTIONS

Small scale digital device forensic tools aim to extract data from cell phones, smart phones, PDAs, and GPS devices. These tools consist of both hardware and software components and come with a diverse range of connectors.

Mobile forensics tools typically are expensive. My advice to you is to buy one of the following products for the sake of demonstration in the lab:

8.1 Paraben's Mobile Field Kit

Paraben's Mobile Field Kit [15], is a portable handheld forensic solution. The kit includes everything you need to perform a comprehensive digital forensic analysis of over 4,000 cell phones, PDAs, and GPS devices anywhere, anytime. Better yet, you can use your Device Seizure dongle that comes in the kit on any lab machine making it more than just a field kit.

8.2 Oxygen Forensic

Oxygen Forensic Suite 2012 [16], is a mobile forensic software that goes beyond standard logical analysis of cell phones, smart phones and PDAs. Using advanced proprietary protocols permits Oxygen to extract much more data than usually extracted by logical forensic tools, especially for smart phones.

8.3 XRY

XRY Complete [17], is the all-In-one mobile forensic system from Micro
Systemation; combining both logical and physical solutions into one package. XRY Complete allows investigators to practice all various existed methods in order to recover data from a mobile device.

9 ISSUES AND CHALLENGES

The need for computer forensic jobs is only expected to increase. There are four different types of computer forensic jobs: law enforcement, consulting, financial, and academic. Computer forensics professionals have specialized skills in data retrieval, analysis, systems integration, and security software.

There are certain factors you need to think about and consider when you building your digital forensics lab. Firstly, you need to have some variation when you choose digital forensics analysis software and tools. If you have a good budget, then we recommend that you purchasing more than one multipurpose digital forensics analysis software. This software should be recognized as court-validated standard in computer forensics software. It should have good support and training available. Secondly, do you really need to go with the option of building a virtual digital forensics lab? Virtual environments for the digital forensics lab still have some issues that need to be resolved such as usage of: software write blocker, licensing dongles, and some hardware items for small scale digital device [18,19]. Finally, whether to use free open source analysis software tools or licensed close source ones? Open source analysis software tools are free but useless when your findings as a digital forensic investigator are going to be used in a court of law.

Finally, The National Institute of Standards and Technology (NIST) launched the Computer Forensic Tool Testing (CFTT) project [20]. It helps different interested parties in making informed choices about acquiring and using digital forensics tools. Moreover, It provides test material for proficiency testing and digital forensics lab-based tool testing.

10 CONCLUSIONS

Many educational institutes started to offer Digital Forensics and Cyber Security as a separate degree or specialization to meet the market high demand. Digital Forensics education is based on vast amount of experiments and laboratory work. This paper explores various items and products that is needed in order to build a Digital Forensics Lab. Graduates of Digital Forensics program need to be one step ahead thinkers of criminals in order to fight against crimes. The specifications and hardware requirements for the lab will vary depending on your budget and the type of media you will examine during your investigation.

11 REFERENCES


