AC 2009-1123: COMPUTER FORENSICS: SEIZING AND SECURING DIGITAL EVIDENCE

Saleh Sbenaty, Middle Tennessee State University

Dr. Saleh M. Sbenaty is a professor of Computer Engineering Technology, earned his Ph.D. and MS degrees in electrical engineering from Tennessee Technological University and his BS degree in electrical engineering from Damascus University. Dr. Sbenaty joined MTSU in 1993 and has been teaching graduate and undergraduate courses in electronics and computer harware. He is actively engaged in curriculum development and assessments for technological education. He has authored and co-authored several industry-based case studies and participated in three major NSF-funded Advanced Technological Education grants over an eight-year period. He also served as the Coordinator of the Computer Engineering Technology program for more than six years. Dr. Sbenaty published and presented over 30-refereed national and international articles and attended/conducted over 60 workshops. He is also conducting research in the area of mass spectrometry, biosensors, electrical characteristics of concrete, and instrumentation. Dr. Sbenaty has several years of industrial and research experiences with Oak Ridge National Laboratory, Lockheed-Martin, and TVA. Dr. Sbenaty served as a Guest Editor and on the Editorial Board, Journal of SMET Education: Innovations and Research. He is currently serving as a program evaluator for the Accreditation Board of Engineering and Technology, ABET.

Stan Mitchell, LogicForce Consulting, LLC

Stan Mitchell is the Forensic Lab Manager at LogicForce Consulting, LLC, a legal technology consulting firm in Nashville, Tennessee, where he conducts computer forensic examinations in civil litigation. Stan served over twenty years in Law Enforcement working as a Patrol Officer, Detective, and Instructor at the Metropolitan Nashville Police Department. He also implemented and operated the Metropolitan Nashville Police Department's Computer Forensic Lab from 2000-2005. In his career, Stan has conducted over 200 forensic analyses, ranging from intellectual property theft to homicide investigations. He is qualified as an expert in Computer Forensics in local, state, and federal courts and has testified in criminal and civil matters numerous times. Credentials: Certified Forensic Computer Examiner (IACIS), 2001; Certified Electronic Evidence Collection Specialist (IACIS), 2001; Certified Computer Forensic Instructor (IACIS), 2004; EnCase Certified Examiner – Guidance Software, 2006; Training Committee member, Coach, and Trainer for IACIS. Qualified as an expert witness in Computer Forensics.

Hugh Berryman, Middle Tennessee State University

Dr. Berryman received his M.A. and Ph.D. in Anthropology from the University of Tennessee, Knoxville, and is certified by the American Board of Forensic Anthropology. Currently, he is a research professor with the Department of Sociology and Anthropology and Director of the Forensic Institute for Research and Education at Middle Tennessee State University. He served on the faculty of the Department of Pathology, University of Tennessee, Memphis, and as Director of the Regional Forensic Center, Memphis, Tennessee from 1980 to 2000. While in Memphis, he taught as an adjunct professor in the Department of Anthropology and the Department of Criminal Justice at the University of Memphis, and provided lectures at the Smithsonian Institute, the Armed Forces Institute of Pathology and the Tennessee Law Enforcement Training Academy, Nashville. In 2000, he began a forensic anthropology consulting business and was Associate Director of the Southern Institute of Forensic Sciences until 2005. During this time he co-taught courses at the University of New Orleans, Colorado State University, and Missouri Western. Dr. Berryman provides forensic anthropology consultation to the Joint POW/MIA Accounting Command Central Identification Laboratory in Hawaii (U.S. war dead identification), and the Office of the Tennessee State Medical Examiner. He is serving his third term on the Board of Directors for the American Board of Forensic Anthropologists. His research interests include physics of bone fracture and fracture interpretation, and he has published in excess of 50 articles in scientific journals and as chapters in books.

Computer Forensics — Seizing and Securing Digital Evidence

I. Abstract

The current paper focuses on the importance of properly seizing and securing digital evidence and the need to educate law enforcement personnel with the correct methods of collecting, documenting, packaging, labeling, and protecting computer related evidence. The paper presents an overview of computer related crimes, computer forensics, and the proper procedures for seizing and securing digital evidence. A description of a short course that was designed to provide law enforcement and forensic personnel with the knowledge needed to collect and preserve digital evidence, and the results gained from this experience are also provided.

II. Introduction

Computer related crimes are steadily increasing at an alarming rate. Digital evidence, as with any evidence, must be preserved in its original state. The law requires that evidence be authentic and unaltered. For digital evidence to be successfully utilized in a criminal investigation, no spoliation to that evidence should occur. A major aspect of preserving digital evidence is collecting it in a way that does not alter it. Computer forensics involves the preservation, identification, extraction, and documentation of digital evidence in the form of magnetically, optically, or electronically stored media (J.P. Craiger 2005). Therefore, law enforcement agents nowadays face a new challenge; they must be familiar with the proper procedures of seizing and securing digital evidence.

1. Computer Forensics

Computer forensics may be defined as the retrieval and analysis of data from a seized computer or any other electronic media performed in such a manner that the results are reproducible by another examiner who, by following the same steps, reaches the same conclusions. Computer forensics has also been described as an “electronic autopsy” of a digital media, because specialized training and hardware/software tools and techniques are all required to make an exact image/copy of the drive. The retrieved data is then analyzed along with the various levels at which that data is stored.

2. Computer Crimes

Computers and digital media have become integral parts of our lives. In 1997, the US Census estimated that only about 18% of households in the US had computers. In 2000, this number grew to 51% with 42% of those households having Internet access. In 2003, the number has increased to 62% of households with 52% having Internet access. Currently, almost 90% of households in the US have computers. Therefore, crimes committed on computers are no longer limited to skinny guys with pimples, a tape on their glasses, and squeaky voices. Almost anyone nowadays can point, click, and use a computer to commit just about any crime. So what type of crimes are being committed using computers? What information is generated to corroborate the facts and circumstances and help in the crime investigation?

A better question to ask would be: What crimes are not being committed with the help of computers? Which investigations could not involve a computer?

- Burglary
- Auto Theft
- Identity Theft
- Embezzlement
- Fraudulent use of Credit Cards
- Domestic Violence
- Stalking
- Bomb Threats
- Hacking
- Prostitution
- Gambling
- Narcotics
- Money Laundering
- Counterfeit Checks
- Homicide
- Suicide
- Child Pornography
- Child Exploitation
- Missing Persons
- Piracy of copyrighted materials

And the list continues to grow on a daily basis!

3. Types of Digital Forensics

There are mainly three types of digital forensics. These are:

a. Computer Forensics
   - Computers (internal and external hard drives).
   - Diskettes, CDs, DVDs, cartridges, and tapes.
   - Thumb drives, flash media, and memories.

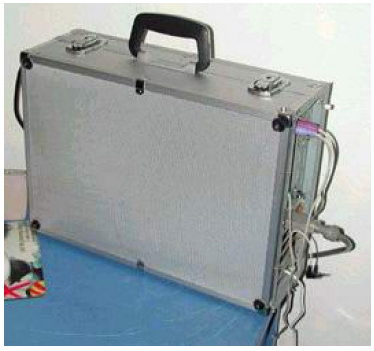
b. Network Forensics
   - Routers
   - Servers
   - Switches
   - Hubs
   - Cards
   - Firewalls
   - Bridges
   - Logs

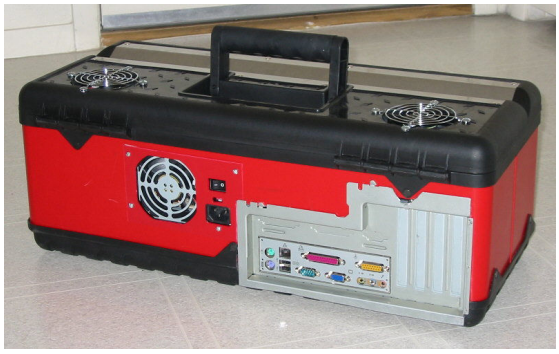
c. Digital Forensics (Specialties)
   - PDA's
   - Cell phones
   - IPods, MP3 players, GPS, etc.

Digital forensics require from investigators special computer software and hardware skills that include but not limited to understanding: operating systems (artifacts), file systems (structures), computer software, hardware, networking, and basic electronics and communication. Moreover, investigators should know how to handle "evidence" and possess good research, writing, and troubleshooting skills in addition to self-motivation.

4. Proper Seizure of Digital Evidence

Collecting digital evidence is quite involved since data might be altered easily. There are general standard procedures that must be followed for each type of digital evidence such as powering down or isolating the equipment. However, each situation presents a unique challenge since no two cases are the same. When seizing a PC, for example, law enforcement personnel usually confiscate the computer, any external storage devices, all floppy disks, zip disks, CD's, DVD's, and other loose media, all books and manuals pertaining to the system, ISP invoices, paper information that may be on or around the computer, including "sticky notes" that may contain passwords, and any unusual adapters/dongles or other hardware directly connected to or located near the computer. Sometimes, computers can be disguised; however, skilled officers are trained to recognize such equipment.





When seizing powered devices such as PDA's and cellular phones, it is important to seize the power supply/charger/AC Adapter since there are many different models available. If battery power is exhausted, data is usually lost unless power is provided. The battery is usually never removed from the phone, which is plugged into power as soon as possible. These portable electronic devices should be isolated from communication signals as soon as feasible.

III. Forensic Institute for Research and Education

The Forensic Institute for Research and Education (FIRE, www.mtsu.edu/fire) at Middle Tennessee State University (MTSU) was created in 2006 to provide exceptional training opportunities for law enforcement and forensic personnel as well as to foster state-of-the-art forensic research. As a part of the Institute educational activities, a short course designed for law enforcement personnel and titled "Seizing and Securing Digital Evidence" was developed and approved by the Peace Officer Standards and Training Board (P.O.S.T). The course, which included a hands-on component, was held on February 8, 2008 and was co-sponsored by FIRE and the College of Continuing Education and Distance Learning, both at MTSU.

The eight-hour course was designed to provide the participant with the proper methods/procedures for seizing and securing digital evidence, computer components, and other related high-tech equipment in computer related investigations. With the completion of this course, the participants were able to:

1) Gain a basic understanding of Computer Forensics, and its abilities to assist in criminal investigations.
2) Recognize the types of criminal activities in which digital evidence is currently being utilized.
3) Recognize computer hardware, digital media, and other high tech. components.
4) Have a basic knowledge of "stand-alone" computer seizures and documentation.
5) Practice proper packaging, labeling, and protecting computer related evidence.

There were 24 participants enrolled in the course. All those who took the survey at the end of the course indicated that they would recommend it to their colleagues and felt that the course was very valuable. Most of the participants were law enforcement personnel, two of whom were from MTSU Public Safety.

The news of the successful short course spread quickly and resulted in a partnership with the Middle Tennessee Chapter of the Association of Certified Fraud Examiners, ACFE. As a result, a half-day seminar was put together by FIRE associates and presented at the ACFE Middle TN Chapter Annual Meeting on January 12, 2009. The seminar included two sessions: An Introduction to Computer Forensics and Computer Crime, and Seizing and Securing Digital Evidence. The meeting was hosted by Nashville State Community College and attended by over 300 ACFE members. In addition, through this partnership, ACFE scholarships will be made available to MTSU students who are interested in forensics as well as high school students who are interested in attending the CSI Summer Camp at MTSU.

Another important mission of FIRE is to get high school students interested in forensics. A CSI Summer Camp was designed and offered over a three-day period in June of 2007 and 2008. The goals of the CSI Summer Camp at MTSU are to allow rising high school students to explore the many unique career possibilities in forensic science, to provide a "real-life" reason to tackle higher-level math and science courses, and to develop skills in teamwork, seeing and understanding details, critical thinking, problem solving, and communication.

The student investigators are presented with a re-creation of an actual crime scene. They are divided into several teams and each team is assigned a member of the Forensic Search and Recovery Team. A professional will direct and coach the students as they use math and science to solve the crime. Each student is trained in the fundamental process of collecting evidence including DNA, fingerprints, hair and fibers, simulated blood spatter, and shoe prints. Additionally, students learn how to process the evidence, conduct interviews, and formulate theories while working within a team environment. During the last afternoon of the camp, each team makes a presentation detailing their theories of the crime and the conclusions they reach. Team conclusions will be critiqued by a panel of forensic scientists. Parents are welcome to attend the last camp session.

During the CSI Summer Camp of 2008, a session entitled "Computer Crimes: An Introduction to Digital Evidence" was designed and presented to three groups. A total of twenty eight high school students from Rutherford and surrounding counties were introduced to computer crimes as well as to the proper ways for collecting digital evidence during their three-day camp at

MTSU. Several students expressed their interests in pursuing a career in a computer-related filed. The session will be also presented during the 2009 summer camp.

IV. The Computer and Digital Forensics Laboratory at MTSU

The authors are working on grant proposals to establish a hands-on Computer and Digital Forensics Lab (CDFL) at MTSU. The lab will be utilized in three major areas: training, education, and research.

1. Training

The proposed CDFL at MTSU will be used to educate and train law enforcement personnel, prosecutors, judges, attorneys, financial institutions personnel, and personnel of many other governmental and private institutions in the area of digital and computer forensic investigations and the prosecution of high-tech crimes.

2. Education

The CDFL will serve undergraduate and graduate students who are interested in the fast growing and changing field of computer and digital forensics. Students from several departments such as computer engineering technology, computer science, computer information system, and criminal justice have showed interests in taking courses and in the hands-on training related to this high demand field.

3. Research

The CDFL will also be used to support research activities sought by faculty and students as well as law enforcement experts in the field of computer and digital forensics.

Two components to the CDFL are proposed:

A. Main Stationary Laboratory: housed at MTSU, that will be used in the hands-on training as well as in education and research. It is envisioned that various workshops will be held on campus to train the above-mentioned personnel. These individuals will come from many cities and towns in TN as well as the surrounding states and will participate in workshops ranging from a day to several days. The lab will include at least six stations, each costing approximately $25,000 for a total of $150,000 and will include:

1. Forensic Workstation from Digital Intelligence (www.digitalintel.com) - $8000.
2. Laptop with forensic capabilities - $4000.
3. Forensic Software - EnCase by Guidance Software (www.guidancesoftware.com) - $3600.
4. Forensic ToolKit by AccessData (www.accessdata.com) - $3900.00
5. Forensic Duplicator - HardCopy3 (www.digitalintel) - $1600.00
6. Forensic Write Blockers - UltraKit (www.digitalintel) - $1500.00
7. Assorted peripherals - USB drive trays, adapters, hard drives CD/DVDs, etc...

8. Other forensics software/hardware.

B. Moving Laboratory: housed in a van, will include at least two training stations, presentation equipment, and will be driven from town to town across the state of Tennessee, and possibly surrounding states, in order to train local law enforcement officers who for various reasons cannot attend the workshops at MTSU. The estimated cost of the van and equipment will be approximately $200,000.

V. Summary and Conclusions

Computer forensics is a fast changing, challenging, and very important field. Computer crimes are on the steady rise; therefore, training and educating law enforcement personnel about the proper handling of such crimes are required. Recruiting students to major and specialize in computer and digital forensics will ensure the proper prosecution of "digital crimes." The Forensic Institute for Research and Education (FIRE) at Middle Tennessee State University (MTSU) was created in 2006 to provide exceptional training opportunities for law enforcement and forensic personnel as well as to foster state-of-the-art forensic research.

VI. Recommended Readings and Resources

1. *Digital Evidence & Computer Crime*, Eoghan Casey, Academic Press, 2004.
2. *Computer Forensics – Incident Response Essentials*, Warren G. Kruse, II , Jay Heiser, Addison-Wesley Professional, 2001.
3. *EnCase Computer Forensics – The Official EnCE, EnCase Certified Examiner Study Guide*, Steve Bunting & William Wei, Sybex, 2006.
4. *File System Forensic Analysis*, Brian Carrier, Addison-Wesley Professional, 2005.
5. *Handbook of Computer Crime Investigation Forensic Tools & Technology*, Edited by Eoghan Casey, Academic Press, 2002.
6. International Association for Computer Investigative Specialist (IACIS) www.cops.org
7. Federal Law Enforcement Training Center (FLETC) www.fletc.gov
8. National White Collar Crime Center (NWCCC) www.nw3c.org
9. SEARCH - National Consortium for Justice Information & Statistics www.search.org/programs/hightech/courses.asp
10. High Technology Crime Investigators Association (HTCIA) www.htcia.org
11. TechnoSecurity – www.thetrainingco.com
12. Encase – www.guidancesoftware.com
13. Paraben – www.paraben-forensics.com
14. Digital Intelligence – www.digitalintelligence.com
15. Access Data – www.accessdata.com
16. NTI – www.forensics-intl.com