Digital Forensic Education & Research Perspective  
Hisham M. Alsaghier, PhD  
College of Computer and Information Sciences  
Majmaah University  
h.alsaghier@mu.edu.sa

Abstract

Information security research focuses on attack before they happen on the system. Digital forensics is related to forensic science deals with the recovery and investigation of material i.e. evidences found in digital devices, related to computer crime. As computer crime grows rapidly, an essential element in improving forensic techniques is development of a comprehensive approach to digital forensics education and research. This paper discusses digital forensic requirements, what exactly do forensic analysts do? How can this type of work help law enforcement or corporate security managers? Also it illustrates steps for forensic investigations, curriculum for digital forensics in Bachelor degrees, Masters Degrees programs along with road map for digital forensic research. Resources and proposed approaches for developing and implementing a forensics program in higher education & research and conclude with a summary.

Key Words: Digital Forensic, Network Forensic, Disk Imaging, cyber forensic

I. Introduction

The term “computer or digital forensics” is originated with early law enforcement practitioners who used the term to refer to the examination of stand-alone computers for digital evidence of all forms of crime. The goal in digital forensic event reconstruction is to sequence all events that are important so that cause–time relationships may be established for an investigation [1].

In early days when network traffic is captured and analyzed, people may describe this as “network forensics” [2]. Over time, the computer forensics process became formalized and commercial tools. Soon, it was recognized that the maturing process should be canonized to allow practitioners to repeat successes and avoid flawed and less-productive processes. Presently, there are several ongoing programs whose goal is to create a comprehensive training and education approach [3]. The CSDS Forensics Workshop is the result of one such effort [4].

Technical aspects divide digital forensic into computer forensics, network forensics, forensic data analysis and mobile device forensics. Before 1980s crimes that involve digital devices were dealt with using existing laws.

II. Background

The collection and analysis of data from computers and other digital devices is required to obtain evidence. Evidence obtained in a Digital forensic investigation is useful in crime, civil, or corporate investigations, but different legal rules may apply. It is important because more than 90 percent of criminals leave evidence which could be captured and analyzed through proper computer forensic procedure. Digital forensics is not just about detective work, it is searching for and attempting to discover information, it also concerned with handling sensitive data
responsible and confidentially, taking precautions to not nullify findings by corrupting data to ensure the integrity of the data and Staying within the law and rules of evidence.

In 1976, Donn Parker’s book, Crime by Computer, was the first book that describe the use of digital information to investigate and prosecute crimes committed with the assistance of a computer. In 1990, Cliff Stoll’s book, The Cuckoo’s Egg [5-6], captures the practice of early digital forensics. In early days Law enforcement officials in USA, Asia, and Europe were struggling with the same problems and making the same personal commitment to prepare themselves and their organizations for the future that they knew was coming. In 1993, the FBI hosted the First International Conference on Computer Evidence at the FBI Academy in Quantico, Virginia, which was attended by representatives from 26 countries. At this conference, it was agreed that the community needed to band together at the agency level to coordinate efforts, share experience and provide assistance to each other. In 1995, the second conference was held in Baltimore and the International Organization on Computer Evidence (IOCE) was founded [7-8].

Digital forensic practice also operated in direct conflict with the traditional laboratory-based practice of forensic science. However, some agencies did see the need for digital forensic capability. The U.S. Secret Service its Electronic Crimes Special Agent Program (ECSAP), the FBI its Computer Analysis Response Team (CART), and the U.S. Air Force Office of Special Investigations its Computer Crime Investigator (CCI) Program and what eventually became the Defense Computer Forensic Laboratory (DCFL). Each agency adopted a different model of selection, training and operations based on its structure and culture.

Traditional forensic laboratories began offering digital examinations. Since 2005, digital forensics has grown in depth and breadth. It has far more practitioners, performing many more examinations of a wider variety, involving ever larger amounts of evidence. In 2006, the United States Courts adopted new Rules for Civil Procedure that defined digital information as a new form of evidence and implemented a mandatory system, called electronic discovery or “e Discovery,” for dealing with digital evidence [9-10].

The workload in traditional law enforcement mushroomed. In Congressional testimony, the FBI announced that its Computer Analysis and Response Team (CART) examined more than 2.5 petabytes of evidence in 2007 alone [11-12]. Digital forensics is important now a days because some criminals are getting smarter in data-hiding techniques such as encryption (scrambling data, such as an e-mail message, so that it cannot be read if intercepted in transit) and steganography (hiding a message in a larger file, typically in a photographic image or sound file) can put evidence of criminal activity where traditional search methods cannot find it.

### III. Steps for forensic investigations

Four important phases namely collection, examination, analysis and reporting are the common steps for all forensic investigations. In collection phase collect the data and physical evidence related to the incident being investigated, the examination phase identify extract relevant information from the collected data using appropriate forensic tools and techniques to maintain integrity of the evidence. While in Analysis, Analyze the results of the examination to generate useful answers to the questions presented in the previous phases. Finally in reporting phase, report the results of the analysis, including Findings relevant to the case [13].

In Collection phase while investigating, investigate Identity theft, Fraud, Software piracy and hacking, domestic violence, Terrorism and national security, Theft of intellectual property and
trade secrets etc, also Evidence that can be recover are Computer Fraud Investigations, Accounting software and files, Credit card data, Financial and asset records, Account data from online auctions ,E-mail, notes, letters, User-created directory and file names to classify images etc, Internet protocol (IP) addresses, Text files and other documents containing sensitive information such as passwords. Evidences are something that tends to establish or disprove a fact.

There are four types of evidence, Real evidence, Documentary evidence, Testimonial evidence and Demonstrative evidence [14]. Real evidence is something you could actually carry into court and show to a jury. Documentary evidence is any evidence in written form. Testimonial evidence is the statement of a witness, under oath, either in court or by deposition. Demonstrative evidence recreates or explains other evidence. Evidences are Admissible, Authentic, Complete, Reliable and Believable. Forensic methods should eliminate alternative suspects and explanations until a definite conclusion is reached.

The “Best Evidence” Rule says that Evidence presented in court should be original and the actual item investigated or examined (and therefore considered “best evidence”). A proper forensic image can be considered Best evidence if the original evidence has been returned to its owner[14].

The Daubert Test, The Case of Daubert v. Merrill Dow Pharmaceuticals established new criteria to determine the reliability, relevancy, and admissibility of scientific evidence [15]. The Daubert Test says that The theory or technique must have been tested, and that test must be replicable. The theory or technique must have been subject to peer review and publication. The error rate associated with the technique must be known. The theory or technique must enjoy general acceptance within the scientific community. Evidence uncovered in a digital investigation may be direct evidence of a crime or might simply corroborate other evidence.

This work should be done by forensic experts specifically trained and experienced in investigative methods. System administrators and information security professionals should gain enough knowledge to know they don’t have to be forensics experts. They should, however, work to minimize risk to their environment to help in the event of an incident.

IV. Ethical issues

The digital forensic investigator must maintain absolute objectivity. It is not the investigator’s job to determine someone’s guilt or innocence. It is the investigator’s responsibility to accurately report the relevant facts of a case. The investigator must maintain strict confidentiality, discussing the results of an investigation on only a “need to know” basis.

V. Curriculum for Digital Forensics

Digital forensics is multi-disciplinary course, several other fields are also involved, mostly related to criminology, information sciences, and computer engineering. In order to structure the topics in this field, we partition the topics into four categories, the first three relating to evidence: (1) Evidence collection (2) Evidence Preservation and (3) Evidence presentation and fourth category spans the first three by addressing issues that can be done before malicious acts occur that will facilitate the forensics process afterward, (4) Forensic Preparation.

VI. Education Frame Work

The overarching goal of the Bachelor degree and Master degree in Computer Engineering program in University or college is to prepare and train students to analyze the relationship
between computer software and hardware used in academia, business, industry and manufacturing. The program provides students with broad knowledge in selected areas of computer engineering, including computer organization, signal and systems, data transmission, computer architecture, digital signal processing, digital control, computer networks, modeling and simulation, optical networks, network programming, mobile and wireless networks, computer network security, embedded systems, hardware description languages, and computer arithmetic and digital forensics. Students learn to design systems and components, identify engineering problems, communication effectively in a team environment, solve computer engineering problems and understand the impact of computer engineering on the global community.

Computer Forensics bachelor degrees programs generally require several courses like data transmission, digital signal processing, digital control, computer networks, modeling and simulation, wireless networks, computer network security, operating system, information security, embedded systems, data recovery, data mining along with criminal justice, criminal law, digital evidence, cyber law, etc.

Masters degree programs include forensic theory in computer science along with political, chronological and legal frameworks. Master degrees programs generally require several courses like Theory of Investigation, Digital Evidence, System analysis, Computing theories, System security, System Integration Cyber criminology, cyber law, Retrieving and analyzing forensic data etc

Computer Engineering (CE) is an essential element of Digital Forensic. Computer hardware often holds the key to evidence discovery and recovery and computer engineers are best suited to developing suitable techniques and procedures for this task. While computer engineering is an essential component of a Digital Forensic program, forensics applications would represent only a very narrow range of the scope of a CE department.

VII. Tools: Hardware & Software for Digital Forensic

The hardware tools needed for a successful forensic analysis can be divided into two categories, incident response and laboratory. Incident response tools would include the hand tools, cabling, identification supplies, and other items necessary to perform an investigation at the scene of an incident. Laboratory tools would include the devices and accessories necessary to perform an analysis, under controlled conditions, of evidence retrieved from an incident scene.

A modern mobile forensic workstation F.R.E.D. L.(Forensic Recovery of Intelligence Device - Laptop) by Digital Intelligence. The UltraKit by Digital Intelligence, Includes write-blockers, cables, adapters, and power supplies necessary for obtaining evidence during incident response [17]. In the digital forensic laboratory, Forensic workstations are customized computer systems that contain the equipment necessary for analysis of suspect computers In addition to standard PC components such as motherboards, hard drives, and memory, forensic workstations.

There are three generally accepted methods for duplicating hard drives i.e Dedicated forensic duplication systems, System-to-system imaging and Imaging on the original system. **Disk Imaging** on a Dedicated Forensic System built and designed to accommodate numerous types of hard drive connections. Specialized bit-level imaging software transfers an exact copy of
the contents of the original hard drive (or other data source) to one or more blanks. If the forensic analysis is correct, the investigation should produce the same results on identical copies of the drive.

**System-to-System Disk Imaging** method uses two separate computer systems -- the suspect and a specialized forensics imaging system. Depending on the type of drives and connections available, both systems are booted from CD-ROM, DVD, USB drive, or floppy disk which loads the imaging software. This method can be slow, and is often not suited to on-the-scene incident response.

**Disk Imaging on the Original System.** Uses the original (suspect) computer to perform the disk imaging transfer process. A blank drive matching the original hard drive’s capacity and configuration is added to the system.

A forensic boot disk is used to create a bit-level image of the original disk. This method is typically used in on-the-scene incident response when it is impractical to transport a computer to the investigator’s laboratory.

Software used in digital forensic analysis comes in two varieties, Commercial software and Open-source software. In either case, the software is typically used for copying data from a suspect’s disk drive (or other data source) to an image file, and then analyzing the data without making any changes to the original source. The forensic software do Disk imaging, Data recovery, Integrity checking, Remote access, Password recovery, Permanent file deletion and Searching and sorting. Some representative Software’s are EnCase and P2 Commander, Helix, SMART.

**VIII. Road Map for Digital Forensic Research**

The latest Digital forensic analysis and research is focused on assisting the law enforcement community. Existing technologies are in the support of law enforcement as well as assist the courts, including digital forensic evidence. Some important topics/area address Digital Forensic technology challenges are; How to Define a Framework for Digital Forensic Science to faces new challenges, Reliability of Digital Evidence, Detection and Recovery of Hidden Data and Digital Forensic Science in Networked Environments i.e. Network Forensics. Research must address challenges in the procedural, social, and legal field. Since digital technology continues to change so fast investigators difficulty in applying currently available analytical tools. Analytical procedures and protocols are not standardized nor do practitioners and researchers use standard terminology. Privacy of Individual is also an important area in this regards. We can create the most advanced technology possible, but if it doesn’t comply with the law. Training in the area of latest Digital forensic technology is required to train the forensics experts.

**Forensic Analysis Requirements**

Law enforcement requirements focus on gathering evidence for use in prosecution that will be scrutinized against established, strict judicial standards. Business requirements are driven more by economics for use in keeping the business on track using reasonably effective techniques that are cost justified and, more importantly, fast. The academic requirements are still being drafted but should focus on accuracy of result derived from precise, repeatable methods that have wide application to all forensic consumers. All represent a distinctly different approach using varied criteria. Just as important here is the fact that systems must be analyzed while active. In most cases, this is the opposite of the current law enforcement view.
Research must provide answers as to what data can be collected safely on active systems and networks and what data has the most benefit. Until forensic analysis becomes effective enough to anticipate attacks and prevent compromise, there will always be the threat that compromise may force the shutdown of mission-essential digital components.

**Digital Forensic Technologies**

Digital Forensic Technologies can be discussed in two major categories; the first one is what are the fundamental truths of digital evidence and second one is what characteristics must be evident across the board for things we deem to be cyber forensic technologies? Other questions are ,Can digital data itself provide clues to motive of a crime or incident? How we Expend the view of digital forensic from standalone system to network ensuring the security of forensic data? Cyber suspects are key issues facing research, but can digital forensic analysis supply answers to the following questions: Who?, What?, Why?, Where?, and When? Are there ever any cyber witnesses to a cybercrime? These are some of the questions that should be considered by researchers striving to provide useful solutions for near-term use.

Other factors relate to desirable characteristics of the technologies themselves. Words like reliable, precise, accurate, non-reputable, secure, flexible, and inexpensive all make the short list. Researchers must also factor these into concepts, designs, experiments, and prototypes. The use of these technologies begs other questions as well. Where are the approved standards? Did the tools used apply those standards? Does digital forensic analysis employ investigative disciplines that require certification? Were the investigators certified? How is digital evidence integrity assured? Some of these questions go to practice rather than research. But in all cases we must identify and then focus on the fundamentals.Among all the approaches, three types of digital forensic analysis can be applied i.e. Examination of physical media for evidence, examination of software for malicious signatures and examination of security of network and logs [18 ].

Digital forensic research should consider some focus in the following areas: (1) advances in detection and reverse engineering technology; (2) wireless technology, its vulnerabilities, and the forensic indicators that will assist operations personnel and investigators in identifying questionable activity; and (3) continue to work toward the establishment of approved standards and best practices to strengthen the foundation for Digital Forensic Science.

**IX. Challenges**

Due to advances in digital technology and the relative growth digital forensics area resulted challenges Like Complexity problem , Device Diversity, Consistency and correlation ,Quantity or volume of Evidence ,Trust of Audit Trails, Testing and Validation ,Anti-forensics and Unified time-lining problem[19, 20,21].Digital evidences are in raw binary form which is difficult for human beings to understand and interpret and this leads to the complexity problem [19,22].Traditional storage devices are simple for storing small data and image files, now a day’s Video, audio, GIS materials, VoIP systems, are used lead to require more space on disk, forensic digital evidence are large in size and require more space on the disk, Investigators are required to analyze huge volumes of data in isolation in the absence of sufficient automation. [23].
Digital evidences challenges in Forensic Investigation are presented in the papers [24, 25,26,27]. Important challenges are, How to large the image and active disk farms dynamically? How to Encrypted files & Whole drive encryption? , How and when use Steganography and other information hiding techniques? , How can we trust on Evidence elimination tools? .How can we trust audit trails? There are various open hard problems, like Forensic tool testing & validation and Open vs. Close Source. Solutions against anti-forensics techniques are Network attack attribution ,Anonymous VoIP threatening callers, Fighting against online fraudsters , Fighting Against Anti-Forensics in this regards various information hiding and evasion techniques are already in practice like Steganography, Watermarking ,Colluded attacks, digital evidence elimination tools and privacy protection techniques.

X. Summary
Digital forensics is a young and maturing field, many interesting and challenging problems faced by Forensic Experts discussed in this paper. Digital forensics is a multi-staged processed that involves different phases namely collection i.e. evidence acquisition, examination of collected data or evidence using forensic tool kits, and finally reporting the result . Curriculum for Digital Forensics in bachelor degrees, graduate certificate programs and Masters Programs along with the hardware and software tools needed for a successful forensic analysis is discussed in details. In Road Map for Digital Forensic Research, we discussed, How to Define a Framework for Digital Forensic Science to faces new challenges, Trustworthiness of Digital Evidence, Detection and Recovery of Hidden Data and Digital Forensic Science in Networked Environments i.e Network Forensics. Research must be address to face challenges in the procedural, social, and legal field. Training in the area of latest Digital forensic technology is also required to train the forensics experts.

References

1. Florian Buchholz, Brett Tjaden, A brief study of time, digital investigation 4 S ( 2 0 0 7 ) S 3 1 – S 4 2- 2007 DFRWS. Elsevier.
4. Center for Secure and Dependable Software (CSDS) Forensics Workshop, University of Idaho, September 23-25, 2002