Computer Forensics: Is it the Next Hot IT Subject?

Victor G. Williams
School of Information Technology
American InterContinental University
vwilliam@mail.maconstate.edu
Ken Revels
Department Chair (Information Technology)
School of Continuing Studies
Mercer University
1400 Coleman Ave
Macon, GA 31207

Introduction

Digital Forensics is not just the recovery of data or information from computer systems and their networks. It is not a procedure that can be accomplished by software alone, and most important, it is not something that can be accomplished by other than a trained IT forensic professional. Digital Forensics is an emerging science and was developed by U.S. federal law enforcement agency during the mid to late 1980s. It is also the art of detecting, processing, and examining digital fingerprints.

A Formal Definition of Computer Forensics:

- The gathering and analysis of digital information in an authentic, accurate and complete form for presentation as evidence in a civil proceeding or a court of law.

- The term digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator

Computer Forensics Overview

Computer Forensics is the application of computer examination and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crimes or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud, child pornography, disputes of ownership, prevention of destruction of evidence, etc. Computer Specialists can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information. Any or all of this information may help during discovery, depositions, settlements, or actual litigation.

The field of Forensic Science has experienced many changes in the last five years. Technology that was on the drawing board yesterday is now part of everyday criminal investigation. What will the well-dressed forensic investigator be using solve tomorrow's crimes?

Traditional information security research focuses on defending systems against attacks before they happen. Although recent intrusion detection systems can recognize and take action against attacks, comparatively little research focuses on after-the-fact investigation. This is, in part, because network owners are more willing to absorb losses from computer crime than risk their reputations by letting details of their exploited vulnerabilities become public. In spite of this reluctance, interest in after-the-fact investigation and evidence gathering techniques is growing in communities beyond law enforcement.

The term computer forensics has many synonyms and contexts. It originated in the late 1980s with early law enforcement practitioners who used it to refer to examining standalone computers for digital evidence of crime. (Some prefer to call this aspect of computer forensics media analysis.) As computers became more networked, computer forensics evolved into a term for post-incident analysis of computers victimized by intrusion or malicious code. People often describe the former instance, in which network traffic is captured and analyzed, as network forensics. Some have argued that forensic computing is a more accurate term, especially because digital evidence is increasingly captured from objects not commonly thought of as computers (such as digital cameras). Despite this, we use the generic term computer forensics here to apply to both workstation and network-focused forensic disciplines. Occasionally, we use the phrase computer and network forensics (CNF) when discussing these related disciplines as a whole.

A computer forensic scientist can use the left-behind data to trace email to senders, find the owner's family and friends, find the sources of digital images, determine shopping habits, find the owner's address, look for airplane reservations, and so forth. The scenario is rich in questions relating to data mining, inference processing, operating system functions, software engineering, and hardware design.

Understanding computer forensics' history is important to understanding how to develop educational programs for this discipline. Media analysis started as the child of law enforcement necessity; computers found at crime scenes offered clues, but investigators needed help to make the evidence they contained visible. Early computer forensic practitioners often operated without academic education or formal forensic training, and fewer still had experience working in a structured computer forensics environment

The computer security community traditionally has focused on protecting information systems from attack. The forensic techniques used peripherally in the intrusion detection community. Similarly, computer security education only recently arrived on the scene; the US National Colloquium for Information Systems Security Education (www.ncisse.org) first appeared in 1997 and featured its first topic on forensics in 2001. In spite of this neglect, the computer forensics process gradually formalized, and manufacturers developed commercial tools to streamline it. Soon, various communities wanted the process to be canonized to let practitioners repeat successes and avoid flawed or less productive methods.

Currently, several ongoing programs exist whose goal is to create a comprehensive training and education approach the Center for Secure and Dependable Software Forensics Workshop is the result of one such effort.

Forensic science requires its practitioners not only to have the appropriate training and education needed to perform the examination and prove the rigor of the techniques, but also to be able to communicate the results clearly to a court, which often contains a lay jury. Forensic equipment, tools, and techniques must have scientific validation and produce a demonstrably accurate result. To do this, tools and techniques must be used in the context of a validated protocol. Only when all three pieces— people, equipment, and protocols—work together, can we verify the results of a forensic examination.

Forensics Case Study

Let's look at a real-world scenario and how computer forensics plays into it. Late one night, a system administrator (sesame) troubleshoots a network problem. She captures several minutes worth of network traffic to review with a protocol analyzer. While conducting this review, she notices some odd traffic. A user's desktop has sent a well-formed packet to an obscure port on an unfamiliar IP address outside the company's firewall. Shortly thereafter, one of the company's research and development database servers transmits a packet that does not conform to any of the formats the company uses to the same IP address. This intrigues the system administrator, who does a lookup of the IP address; it comes back as one of the firm's competitors. Now, she's not merely curious, she's concerned. She picks up the phone and calls her boss. The boss could say, "Just block that port," and then go back to bed. However, there's a far better way to handle this situation. The boss instructs the system administrator to take immediate steps to preserve the collected packets. He then contacts the company's chief information security officer (CISO) and informs him of the situation.

The CISO recognizes this as a security incident that could compromise the company's proprietary information and trade secrets; it could also involve the employee whose workstation contacted the competition's IP address. Fortunately, this is exactly the kind of incident the company had in mind when it developed the computer forensic annex to its information security plan.

The CISO assigns an incident manager from his organization to oversee the event. The incident manager then contacts the company's general counsel to discuss the various legal issues involved in the investigation. Next, he calls out a forensics technician to collect and preserve the evidence at the system administrator's computer, the employee's workstation, the database server, and the firewall.

After conducting a routine examination of the collected material, the forensic technician notices a substantial amount of proprietary information on the employee's hard drive that he does not appear to need. Moreover, the forensic technician can't identify the mechanism used to communicate with the competitor's computer. Analysis of the server and firewall logs reveals that lots of information transferred from the database server to the competition.

After obtaining the general counsel's approval, the incident manager engages a researcher at a major university to review the examination results and work product. The researcher identifies code on both the employee workstation and the database server that's written to send information from the database server to the competitor's computer on command from the employee's work-

station. This command is determined to be the first and middle name of the employee's oldest daughter.

The incident manager uses the reports from the forensic technician and the researcher to write an incident report for executive management. Based on this incident report, the employee confesses to cooperating with an associate employed by the competition. The general counsel sues the competitor for damages, obtaining a restraining order against the competition and demonstrating the company's aggressive protection of its trade secrets.

An Envisioned Forensic Workforce

In the just-described scenario, people with different skills fill different roles. To form a reasonable computer forensics education, we must identify the skills and positions such an educational program will fill. Many communities are interested in computer forensics:

- Law enforcement organizations need to train officers and administrators
- Industry needs professionals with computer forensic competence as well as specialized computer forensics technicians
- Academia needs personnel that can teach existing computer forensic techniques and research and validate new ones.

Recognizing the needs of the wider legal community is also important: judges, prosecutors, and defense lawyers might not want to learn about forensic computing in detail, but they'd certainly like to be able to understand and evaluate its results. Law enforcement personnel are classic just-in-time learners who prize immediate practical application, especially if it leads to a more efficient investigative process.

Regardless of how technically educated law enforcement professionals are, they rely on human factors in their investigations— a videotaped confession is far more convincing to a jury than the most elegant technical explanation as to why someone is guilty.

Four forensic positions represent a reasonable approach to developing a forensics curriculum. These positions represent a logical partitioning of the workforce, not the existing body of knowledge relevant to computer forensics.

What are Educational Institutions Doing about the shortage of trained people?

Many higher learning educational Institutions have recognized the need for a cross between Information Technology and Criminal Justice students. Some instructions have developed a degree or certificated program to meet that need. The most common name for the course of study is "Computer Forensics". However, other names have been used. (i.e. Information Technology Forensics, Technology Forensics, Cyber Forensics etc.)

There could be some opportunities to develop a minor for universities that have a major in criminal justice. Forensics is the art of employing science techniques that can be used in a court of law. Overall, this paper will look specifically at how college and universities teach their students

how to obtain evidence from computer logs and network logs, preserving the evidentiary chain, and the legal aspects of the search and seizure of computers and any equipment logs that are related to a search and seizure court order.

Several topics will present varying levels of detail on IT Forensics. It is expected that Criminal Justice students will be less familiar with computers and networks but more familiar with the legal aspects of the field. This is why it is critical that these courses be taught by IS instructors. The following areas should be covered based on IS curriculum standards.

- Introduction to Information Technology
  - Computer system components and the Internet
  - How TCP/IP and the WWW was formed
  - The Internet viruses and the hacker subculture

- Intro to Internet Computer Crime and Related Demographics
  - Information Security Fundamentals
  - Network user interfaces
  - Computer crime statistics

- Computers and Internet Crime
  - Crimes involving computers and networks
  - Criminals - hackers and crackers

- Investigations
  - -IS Life Cycle
  - -Security Incident Handling
  - -The criminal investigative life cycle
  - -Legal methods to obtain the computer
  - -Jurisdictions and agencies
  - -Internet e-mail, Internet Relay Chat (IRC)
  - -Internet chat rooms, Spam, and other interactive application
  - -IP addresses and domain names; Investigative methods

- Evidence collection
  - Working with ISPs and telephone companies
  - Exploring computer networks, Internet Servers, and LAN & WAN network logs
  - Digital Evidence at the Transport, Network, Data-Link, and Physical Layers

- Legal issues
  - Constitutional law
  - Search and Seizure Guidelines
  - Case Law

- Privacy Protection Act (PPA)
  - Electronic Communications Privacy Act (ECPA)
  - Seizing Electronic Evidence

Investigative and Testimonial Challenges
Future challenges
CALEA
International Computer Crime Laws
Using Digital Evidence as an Alibi

- IT Forensics
  - Types of computers (cars, watches, laptops, PDAs)
  - Operating System file-storage techniques
  - Handling computers and media - maintaining the integrity of evidence collected
  - Searching and retrieving files
  - Intro to Encryption
  - Forensics Application Tools (EnCase, netstat, ping, Sam Spade, trace route, whois, WinHex)

- The Future of IT Forensics
  - Education
  - National Recovery Teams
  - Information Sharing
  - Social Engineering

Below are some of the Educational Institutions that have developed course work and degrees in Computer Forensics.

Anne Arundel Community College, Arnold, MD

- **Cyber Crime Studies Institute**

Blue Ridge Community College, NC

- **Cyber Crime Investigations**

Canyon College, Caldwell, Idaho

- **Introduction to Computer Forensics (Online course)**
- **Law Enforcement: Breaking the Technological Barrier Certificate Program**

Capitol College, Laurel, MD

- **Master of Science in Network Security**
- **Security Management Certificate**

Champlain College, Burlington, VT

- **Computer & Digital Forensics Program**

Clayton State College, OH

- **Criminal Justice - Cybercrime Program**

Cleveland State University, OH

- **CyberForensics Course**

College of San Mateo, San Mateo, CA

- **Computer and Network Forensics Associate Degree**

Community College of Denver, CO

- **Public Security Management Degree**

Cranfield University, Wiltshire, UK

- **Masters in Forensic Computing**

Curry College, Milton, MA

- **Certificate in Computer Crime Investigations & Computer Forensics**

Curtin University of Technology, Western Australia

- **Computer Forensics**

Defiance College, Defiance, Ohio

- **Computer Forensics Major (BS)**

Eastern Michigan University, Ypsilanti, MI

- **Information Assurance Training**

Edmonds Community College, Business & Technology Center, Everett, WA

- **Introduction to Computer Forensics**

Fairmont State College, Fairmont, WV

- **Minor or Certificate of Completion in Computer Forensics** [PDF]

Fleming College, Ontario, Canada

- **Computer Forensics Training (on-line)**
- **Computer Security and Investigations (CSI)**

Fond du Lac Tribal and Community College, Cloquet, MN

- **AAS in E-Crime Investigation** [PDF]
- **Computer Forensics Certificate** [PDF]

George Washington University

- **Graduate Certificate in Computer Fraud Investigation**

Glouster County College Police Academy, Sewell, NJ

- **High Technology Investigations**

Goodwin College of Professional Studies, Philadelphia, PA

- **Computer Forensics; Information Warfare courses**

Hong Kong University of Science & Technology
- **Graduate & Professional Diplomas in Computer Forensics**

ICM School of Business & Medical Careers, Pittsburgh, PA
- **ASB Degree in Criminal Justice - Cybercrime**

Iowa Lakes Community College, Emmetsburg, IA
- **Associate in Science of Computer Forensics**

Iowa State University, Ames, IA
- **Computer and Network Forensics**

James Madison University, Harrisonburg, VA
- **Computer-Related Law and Computer Forensics Course**

Overland Park, Kansas
- **Intro to Computer Forensics**

Lake Washington Technical College, Kirkland, WA
- **Computer Forensics and Security AAS & Certificate**

Leigh Carbon Community College, Schnecksville, PA
- **Computer Forensics Courses**

Maricopa County Community College, AZ
- **Cyber Forensics Technician Certificate**

Marshall University Graduate College, WV
- **MS Forensic Science Program**

Medaille College, Buffalo, NY
- **CJ Concentration in Computer Crime Investigation (BS)**

Melbourne University Private, Australia
- **Graduate Certificate in E-Crime Investigation** [PDF]

Miami Dade College, Miami, FL
- **Computer Forensics & Investigation Program**

Mississippi State University, MS
- **Computer Crime and Forensics Course**

Missouri Southern State University, MO
- **Bachelor of Science in CIS and Bachelor of Science in Criminal Justice - Computer Forensics Option**

Andrea Han	Miami University Middletown	8
Tim Hall	University of Indianapolis	8, 251
Sam Hijazi	Florida Keys Community College	125
Laurie Hillstock	Clemson University	138, 139
Janet Hurn	Miami University Middleton Campus	146
Mary Insabella	Columbus State Community College	151
Frederick Jenny	Grove City College	157
Geraldine Covert Jenny	Slippery Rock University of Pennsylvania	161
Elizabeth Kiggins	University of Indianapolis	8, 251
Michael Kress	College of Staten Island CCNY	184
Steven Krohn	North Dakota State College of Science	168
Tom Kruse	Loras College	174
Lynda LaRoche	Depauw University	94
Jay Lee	Philadelphia Biblical University	31
Mark Lecher	Franklin College of Indiana	180
Mark Lewenthal	College of Staten Island CCNY	184
Robert Mainhart	Saint Francis University	190
John Nelson	Pikeville College	196
Shirley Nelson	Pikeville College	196
Laurie Patterson	University of North Carolina at Wilmington	197
Constance Pender	University of South Carolina-Sumter	63
Thomas Pollack	Duquesne University	207
Mark Poore	Roanoke College	217

Cheryl Reindl-Johnson	Sinclair Community College	9
Eric Remy	Randolph-Macon Womens's College	218
Ken Revels	Mercer University	261
James Roberts	Charleston Southern University	46
Gary Rogers	Macon State College	229
Pat Schultz	University of South Carolina-Sumter	63
Michael Shanafelt	Saint Francis University	105
Jeanne Skul	Loras College	174
M. Leigh Smith	Florida Keys Community College	125
Robin Snyder	Savannah State University	230
Lisa Spence	Georgia Southern University	240
Carmen Springer-Davis	Casper College	9
Nesan Sriskanda	Claflin University	241
Dewey Swanson	Purdue University School of Technology	242
Nancy Thibeault	Sinclair Community College	250
Nate Tucker Sr.	Lee University	8
Anne Vaassen	Loras College	174
George Weimer	University of Indianapolis	8, 251
Victor Williams	American Intercontinental University	261
Fred Worthy	Charleston Southern University	46
Carol Yackel	Mercer University	85

Network Technology and Exchange Center, Hong Kong

- **Computer Forensics Analysis Seminar**

North Carolina Wesleyan College, Rocky Mount, NC

- **Course in Computer Forensics**

Northeastern University, Boston, MA

- **Certificate of Professional Achievement - Communications & Networking**
- **Graduate Certificate in Network Security Management**

Northern Virginia Criminal Justice Training Academy, Ashburn, VA

- **Technology Investigation Courses**

Norwich University, Northfield, VT

- **Introduction to Computer Forensics**

Oklahoma State University

- **Bachelor of Technology - Information Assurance & Forensics**

St. Ambrose University, Davenport, IA

- **Minor in Computer and Network Security**

St. Petersburg College, FL

- **Computer Related Crime Investigations Certificate**

Stark State College of Technology, Canton, Ohio

- **Computer Network Administration and Security Technology Security & Forensics Option**

State University of New York (SUNY) Farmingdale

- **B.S. degree program in Security Systems**
- **SUNY Learning Network Online (Distance) Learning - Courses in Computer Forensics**

Presenters' Index