Computer Forensics Education

Alec Yasinsac[1], Robert Erbacher[2], Donald G. Marks[3],
Mark M. Pollitt[4], Peter Sommer[5]

Abstract

While research is exploding on information security, the need for application of science and education to forensics for computer related crimes is largely limited to law enforcement organizations. At the recent Workshop on Computer Forensics, there was extensive discussion of requirements and approaches to developing a workforce for computer forensic investigation. We present results of those discussions in this paper.

Keywords: Computer Forensics, digital evidence,

1. Introduction

Traditional information security research focuses on defending systems against attack before they happen. More recently, security auditing has evolved to intrusion detection systems that are concerned with recognizing attacks and taking action to curb further damage at the time of the attack. Comparatively little research has focused on after the fact investigation, partly because network owners are willing to absorb losses from computer crime rather than risking their reputation by allowing details of their exploited vulnerabilities to become public.

In the face of growing losses resulting from computer crime, interest in after the fact investigation and evidence gathering techniques is growing. An essential element in improving forensic techniques is development of a comprehensive approach to forensics education. In this paper we present requirements, resources, and proposed pedagogical approaches for developing and implementing a forensics program in higher education. In the next section we address the composition of a forensics workforce and follow with a discussion of curricula issues. We then present arguments for finding suitable resources for a forensic education program and conclude with a summary and recommendations.

2. Background.

The term “computer forensics” is used in many contexts and has many synonyms. The term 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. Some prefer to call this aspect of computer forensics by the term “media analysis”. As computers became larger and more networked, computer forensics became a term commonly used to refer to the post-incident analysis of computers victimized by an intrusion or malicious code. Particularly in the former instance, where network traffic is captured and analyzed, people may describe this as “network forensics” [1].

Some have argued that “forensic computing” is a more accurate term for either of these scenarios, especially since more and more digital evidence is being examined from objects not commonly thought of as computers (i.e. digital cameras). Despite this, we will utilize the generic term *computer forensics* to apply to both workstation and network-focused forensic disciplines. Occasionally, we also use the phrase *Computer and Network Forensics or CNF* when discussing

these related disciplines as a whole. Data of analytical value will often be found in both its dynamic state (network traffic) and its static state (media).

It is important to understand the history of computer forensics in order to understand how educational programs might be developed in this discipline. Media analysis was the child of law enforcement necessity. Computers were being found at crime scenes and investigators were eager to use this new source of information. The investigators sought out people to assist in making this latent form of evidence visible. Often, the few people that were familiar with computers were system administrators of law enforcement systems or other investigators who happened to have either a previous background in information technology or were hobbyists. Early computer forensic practitioners often operated without academic education or formal forensic training. Fewer still had experience working within a structured computer forensics environment.

Over time, the computer forensics process became formalized and commercial tools were developed to streamline the process. Soon, it was recognized that the maturing process should be canonized to allow practioners to repeat successes and avoid flawed and less-productive processes. Localized, ad hoc training programs began to appear out of necessity. Presently, there are several ongoing programs whose goal is to create a comprehensive training and education approach. The CSDS Forensics Workshop [2] is the result of one such effort.

3. An Envisioned Forensic Workforce

In order to form a reasonable computer forensics education approach, we must identify the skills and even the positions that the education program will fill. Many different communities are interested in computer forensics. Law enforcement organizations need to train officers and administrators. Industry needs computing professionals with computer forensic competence as well as specialized computer forensics technicians. Academia needs personnel that can teach computer forensic techniques, research new techniques, and validate new methods. There is a strong need for a broad and diverse computer forensic workforce.

As with most fields of study, there are many potential categorizations of forensics topics. We present four forensic positions as a reasonable approach to developing a forensics curriculum. Our view of these positions was influenced in part by the information assurance workforce development programs triggered and overseen by the National Security Agency [3].

3.1. CNF Technician

The CNF technician position is where the forensics rubber meets the road. Persons in these positions exercise the technical aspects of gathering evidence. They must have sufficient technical skills to gather information from computers and networks. They must understand both software and hardware on host computers as well as the networks that connect them. These technicians execute the tasks that have been traditionally considered to be forensics experts. Certainly, they are that. However, they represent only one of the four forensics positions that we propose.

3.2. CNF Policy Maker

At the other end of the forensics spectrum is the CNF policy maker. This manager and administrator establishes CNF policies that reflect the broad considerations of the enterprise. It is their responsibility to see the impact of forensics in the broader context of the business goals. They make the hard decisions that tradeoff forensics capabilities with issues of privacy, and correspondingly, morale, along with the many other tradeoffs demanded of forensics.

While these administrators focus on the big picture, they must be familiar with computing and forensic sciences. This is the need that a CNF curriculum can fill. While computer familiarity is growing among executives, few senior administrators understand the nature or need for CNF. This portion of the curriculum should stress the multi-disciplinary character of CNF, relating the need for protecting the enterprise to its business goals, while illuminating the technological and critical legal fundamentals that CNF demands.

3.3. CNF Professional

While the forensics technician accomplishes the heart of computer forensics, the CNF professional is the link between policy and execution. The CNF professional must have extensive technical skills as well as broad and deep understanding of legal procedures and requirements. Moreover, they must understand the fundamental enterprise business in order to effectively ensure that the CNF policies are properly executed within the business context.

3.4. CNF Researcher

While CNF has not been fully recognized as an independent discipline, it has clearly surpassed the development status that it enjoyed in the early Internet years, and is the topic of applied research appearing in conferences and in workshops, such as this one, addressing its foundations and technology. Additionally, there is a clear demand for educators that specialize in this area. While CNF professionals may be able to double as trainers for elementary computer and evidence discovery classes, graduate degrees are required to introduce these courses into upper level higher education.

As with its sister discipline of computer and network security, we expect that CNF researcher education will begin with masters programs. It is too soon to tell if CNF research will reach a sufficient basic research categorization to meet the rigid "contribution to knowledge" requirements of doctoral degrees.

4. Curriculum for Forensics

Computer forensics is, by nature, multi-disciplinary, founded in the two otherwise technologically separate fields of computing and law. 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. The 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. We see these categories as supporting, but orthogonal to the CNF positions we describe above, and illustrate the relationship in Table 1

Position	Collection	Preservation	Presentation	Preparation
CNF Technician	d	u	f	f
CNF Professional	d	d	d	d
CNF Policy Maker	f	f	u	f
CNF Researcher	u	u	u	d
f = familiarity, u = understanding, d = deep knowledge				

Table 1

4.1. Evidence Collection

The essence of any forensic science is information. Evidence is nothing more than information that is presented in court. Before it can be presented in court, information relative to the malicious act must be discovered and recovered.

In CNF, information is frequently discovered simply by knowing where to look. Information is the primary business of computers and networks, and information can be found in many places not known to the average user; or even to many computer experts. Forensic investigators can find information hidden in logs, caches, swap files, deleted files, and unwritten segments. In networks, information finds its way into intermediate devices such as router caches, switches, proxy servers, firewalls, and other network devices. It is the unique job of the forensics expert to have broad and deep knowledge regarding the myriad of nooks and crannies where important tips and evidence can be found.

Data recovery, on the other hand, results from applying extraordinary measures to extract information from locations where it is known to reside. The best-known illustration of data recovery is recovering data from electro magnetically wiped or damaged disk drives. Extracting deleted files from magnetic devices or volatile memory is another well-known data recovery area. Not so well known is that network information is rarely available exclusively through discovery. Network information is partitioned into packets that must be reconstructed into sessions in order to recover the relevant information. Discovering and recovering information is the heart of forensics.

4.2. Evidence Preservation

Once information is recovered, there are rigid requirements for preserving it if it is to be later used in court. Still new to the courtroom, procedures for preserving digital evidence are evolving. There are two important questions that CNF experts must be able to answer properly: (1) Was the evidence gathered properly so that it reflected all pertinent information on the subject device when it was collected? (2) Has the evidence been changed since it was collected?

Technology such as secure copying and storage mirroring, provide mechanisms for showing the accuracy of the acquired evidence. Mirroring is simply making an exact copy of an entire storage device. The relevant information can be extracted from the copy without disturbing the original device. Secure copying techniques allow investigators to bind the target information to some other information that can allow verification that the copy is accurate.

Cryptographic digital signatures provide integrity of the evidence. Similar in function to traditional evidentiary chain of custody, these signatures are tamper resistant against even sophisticated intruders and can be reconstructed from the presented evidence to ensure its authenticity.

4.3. Evidence Presentation

Digital evidence is notoriously difficult to present in court. The greatest challenge is that digital evidence has no natural physical character. Rather, digital evidence is very abstract. To further complicate this challenge, while computers are pervasive in society, a good portion of the juror pool has little understanding, and maybe little exposure to computers, networks, or digital information.

Approaches to presenting digital evidence are based on the presentor assuming the juror's view; essentially putting themselves in the jurors's place. They do this by studying case histories and employing simple and sophisticated graphics to make the digital case. Few computer technicians or experts are familiar with the difficulties in presenting evidence in court, or with

mechanisms that can facilitate that process. These techniques must be taught in a comprehensive CNF program.

4.4. Forensic Preparation

Forensics efforts are traditionally accomplished after a malicious act has occurred. As the field has evolved, it was recognized [4] that much could be done to facilitate forensics investigation before any malicious acts occur. In much the same way as surveillance cameras often make the case against shoplifters, electronic mirroring, logging, and marking can help investigators reconstruct malicious acts and trace attackers.

Forensic specialists can implement procedures to mirror important data, log transaction and network information, and mark information that they may not be able (nor desire) to protect from theft. Watermarking technology allows experts to insert irremovable marks that can be used to irrefutably identify stolen information after it is discovered. Forensic preparation techniques are quickly evolving and present an opportunity for instructors to bring a strong research component into the classroom when these topics are presented.

5. Education and Training

As we have shown, there are a wide variety of topics that must be included in a comprehensive CNF curriculum. Many of these topics are clearly educational, reflecting an appropriate level of academic abstraction to be considered foundational knowledge. Conversely, many of the topics may be considered more skills oriented, and, thus, better suited to presentation in a training program.

The computer security field is represented across the training and education spectrum, with short course skills classes taught by industrial providers, technical schools with one and two year programs, community colleges, undergraduate programs, and graduate degrees to the doctoral level. We posit that a similar structure is appropriate for a comprehensive CNF workforce.

There are many different ways to characterize the differences between training and education. Some are given in Figure 1.

Training----------**Education**

Skills----------Knowledge
Application----------Abstraction
Using tools----------Developing tools
Applying procedures---------Establishing procedures
Practice----------Theory

Figure 1

The distinction may be illustrated by considering the role of tools in CNF investigations. Information discovery and recovery are tool-intensive functions. CNF technicians use tools to examine computers and networks from many different perspectives. Some of these are common tools for system administrators, while others emphasize report-writing skills, and still others provide strong artificial intelligence and data mining features. While it is important to understand the investigative procedure, it is not essential that the technicians understand the internal operation of the tools. The emphasis in not on the tool detail, but what the tool reveals about the data and its underlying structure.

Conversely, the tool builder must have broad understanding of the forensic process, as well as sufficient technical breadth and depth to be able to construct usable tools. They must

understand the technical requirements of the tool input and output as well as the way the technicians expect to use them.

5.1. Undergraduate Education

Computer forensics, as opposed to general computer security, is well suited to undergraduate classes. While there are certainly some outstanding research questions in the field, there is a large body of expertise, techniques, and knowledge than can be presented to undergraduates. In fact, the lessons learned through a computer forensics class will serve undergraduates well in various computer specialties.

One of the fundamental objectives of undergraduate education is to prepare graduates for employment. As the criminal element in society learns to use computers for their personal and professional activities, police departments at all levels will increase their hiring of computer forensic experts. Similarly, the legal defense community, both the defense lawyers and expert witnesses, will need to expand their base of expertise in order to defend clients.

Undergraduate programs can provide an ideal venue for training forensic technicians with the technical skills to discover and preserve CNF evidence as well as providing a closely related program that gives forensic professionals the breadth and multi-disciplinary information that they need to oversee CNF programs.

Computer forensics provides training not only for law enforcement personnel who have seized a computer, but also for system administrators who may need to investigate employee use of company computers. For example, a system administrator may suspect that an employee is using company assets for personal business, seize the computer, and analyze the data to determine if this is occurring. While this is an administrative, not criminal, offense, the data examination requires the same technical expertise. Computer forensics is also extensively used in the *data recovery* business, another area of information technology that can be expected to grow in the future.

Computer forensics classes must cover an in-depth analysis of several software systems including operating systems, e-mail servers, and web browsers. Computer forensic workers must know where to go for information, where operations history is maintained, how files are deleted and recovered, and numerous other questions. This decomposition of software packages will aid their understanding of how large projects are built, how individual programs interface with the operating system and other applications, and how data can be analyzed independently of the application using or creating that data. All of these skills will serve the undergraduate well in future classes and in their employment upon graduation.

Finally, undergraduate programs offer system development skills that are essential to the CNF process. By using rapid prototyping processes for building user interfaces, reusing existing components, and incorporating freeware and shareware into local development processes, CNF professionals can quickly construct helpful tools on the fly.

5.2. Finding a Home for an Academic CNF Program

Because of its multi-disciplinary character, it is unclear where a computer forensics course fits best within the university. This is complicated because of the rapid growth and focus of computing-related disciplines and departments in Universities. Many different computer-related departments have surfaced in recent years, going by such names as Information Sciences, Information Systems, Management and Business Information Systems, Information Technology, et al. The essence of all these departments is that they provide a backdrop suitable for providing

the computer-related training that is essential to a CNF curriculum. For ease of reference, heretofore, we refer to this group of departments as Computing Sciences.

In addition to computing science, several other departments in an academic college or university may argue that their department is best suited to a CNF program, lead by the criminology or criminal justice departments. Their argument is that forensics of any type is no more than a tool of law enforcement. Unfortunately, Criminology and Criminal Justice departments frequently do not have the expertise or resources to offer a computer based course, especially one that utilizes a laboratory.

In addition to the elements we have already discussed, we also consider broader, more conceptual themes. One feature that distinguishes "computer" forensics from other branches of forensic science is the speed of change in Information Technology as a whole – the rate at which new hardware platforms, operating systems, integrated environments, applications and so on appear, and these changes produce cultural changes in the way in which computers are used. Even in the last two years we have seen a considerable growth in the use of peer-to-peer infrastructures, for example. These changes may take place more rapidly than the steady process of peer-reviewed article and syllabus development allow; any rounded education in this area needs to invite students to think how we should address the problem.

A further important conceptual issue is "how far do we take any individual forensic examination?"; in most real life situations forensic resources are limited and their deployment must be related to likely results. How do we balance this against a computer engineer's natural desire never to be satisfied with anything less than the best?

Finally, Computer Engineering (CE) is an essential element of CNF. 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 CNF program, forensics applications would represent only a very narrow range of the scope of a CE department.

A well designed, integrated computer forensics program should appeal to all these departments, and can be expected to draw students from any of them. In fact, even single courses may be interdisciplinary, with participation of faculty from different departments.

5.3. Case Study I: Central Michigan University

Courses in computer forensics are not widely offered in academia. The decision to offer such a class at Central Michigan University offers some insight into the interest, requirements and difficulties of starting up a new program of this type.

First, there is a lot of student interest in the class. Especially in the wake of 9/11, there is a hunger to contribute something to the war on terrorism. Even though the class is focused upon general criminal activity, the students explore technologies that could be utilized in the war on terrorism. The class has a feeling of realism, problem solving, and some play-acting, which is missing in many academic settings.

Students joined special study groups to investigate CNF related issues. Initially, this group studied various cryptography implementations, but then expanded to study steganography, theoretical cryptography, and specialized forensic hardware. The students usually meet in the evenings, but some actually have decided to meet on Saturday mornings. These are undergraduate students doing this in addition to their full load of studies.

This enthusiasm is not limited to the students, the school has responded to their interest by offering a Computer Forensics special study course and purchasing special hardware and software for the course. The grants office, the congressional affairs office, the development office, the operational Information Technology department and the Information Systems (i.e. the library) became aware of computer security and forensics.

The input of these various interest groups should not be overlooked. Each group or department contributed their unique viewpoint and expertise toward making the program more relevant and complete. Each person included in the planning became an advocate to other faculty, staff and students, and the program continued to expand.

5.4. Case Study II: Experience in the United Kingdom

The UK discovered "computer crime" and "forensic computing" quite early. A Computer Crime Unit was set up within the Metropolitan Police (Scotland Yard) in 1985. Today the lead law enforcement body is the National High Tech Crime Unit (NHTCU) that, though police dominated, also includes officers from the military and customs. UK computer forensics products appeared in the early 1990s and for a while Scotland Yard's CCU ran a series of training courses and provided manpower for training at Interpol. The emphasis was heavily practical and orientated towards disk forensics.

Other police forces and law enforcement agencies set up their own training schemes but there was little co-ordination. After a while an informal group of law enforcement officers became subsumed in a Digital Evidence Group run by the Home Office. In the mid-1990s, "short" courses were set up at the Royal College of Military Science (RCMS) at Shrivenham – these were geared towards law enforcement, the military and the security service and they tend to concentrate on the "computer science" and "hardware" aspects of the discipline.

Following a national reorganization of the United Kingdom (UK) Police in 1997, Shrivenham continues to provide the "high end" academic training for law enforcement – a MSc course, not undergraduate, started in 2002. The more vocational forms of training are available from a new specialist center, which provides courses in Network Investigation, Disk Forensics, Computer Forensics for Line Managers and for Child Abuse specialists. Training from product vendors is also available though law enforcement agencies are always anxious to avoid becoming over-dependent on any one product. Training for non-law enforcement personnel is difficult to obtain. However law enforcement have been willing to involve a few defense experts in their deliberations; in the UK the duty of an expert hired by the defense is to the court and not to the defendant.

6. An Academic Forensic Laboratory

Regardless of the composition of the instruction in a CNF program there is wide agreement that any comprehensive curriculum will have an extensive hands on component. Many topics should focus on lab-based instruction, supported by rich software laboratories and equipment to exercise tools, prove concepts, test solutions, and, generally learn by doing. The resources needed to support a comprehensive CNF program fall into the four categories of hardware, software, space, and personnel.

6.1. Laboratory Spaces

Much of the hands-on work required in a CNF program can be accomplished in existing departmental laboratories. In fact, many of the tools that must be exercised can utilize the variety of activity recorded on public machines to their advantage.

Still, there are a significant number of forensic functions that require specialized, dedicated, or segregated components. This necessitates assignment of space for a CNF laboratory. Depending on the size of the program, as few as three desks may be sufficient to handle the workload in such a laboratory.

6.2. Equipment for a CNF Laboratory

Since many CNF projects are similar to other computing sciences projects, they can often be conducted on existing departmental resources, if sufficient laboratory space is available. It is reasonable to assume that a new CFN program will increase the demand and usage of the public computers in the introducing department.

Additionally, there are necessary CNF projects that are not suitable to public laboratories, thus requiring a dedicated and segregated CNF network. The Internet is a highly heterogeneous environment. Thus, a CNF laboratory should sport a wide variety of equipment for workstations, peripherals and network equipment. Workstations should be available in the three most popular operating systems (UNIX[1], Windows™, & Apple™). Network equipment should include hubs, switches, routers, firewalls, proxies, and other network devices that may store information that could be useful in an investigation. To allow flexibility in experimentation, these devices should not be integral components for connectivity of the laboratory. Table 1 lists some devices that could be used in a CNF laboratory.

Computers		Network	Security	Peripherals	Operating Systems	Appli-cations	CNF Tools
Work-stations	Intel™	Routers	Firewalls	Disk Drives	Unix	Office Suites	SNORT
	RISC	Switches	Intrusion Detection	Disk recovery equipment	Solaris	Middle-ware	
	Apple	Proxies		Printers	Windows		
Servers	Intel™			CD recovery	Linux		
	RISC						

Table 2

6.3. Software to Support a CNF Laboratory

As illustrated in Table 2 above, there are three categories of software necessary for a CNF laboratory: (1) CNF tools (2) User operating systems (3) User applications. The tools should be available to be used by students to discover and recover evidence. The operating system software is used to emulate perpetrator and victim machines, and the applications are also used to emulate victim information and processes.

Much of this software is available as freeware, while others are can be attained as shareware or a demo copy used for the project purposes. On the proprietary side, vendors may offer gratis or discounted software for educational use, but there will be a regular demand to acquire specialized software in small volumes for specific experiments.

[1] It may be sufficient to utilize PCs under Linux/BSD, or these operating systems may be additionally represented.

6.4. CNF Laboratory Support Personnel

The final resource that is necessary in a CNF laboratory is support personnel. It is financially appealing to leverage existing technical support staffs to operate and maintain new laboratories. Unfortunately, existing staffs are likely already overtaxed and do not have the specialized knowledge to provide suitable support for a CNF laboratory. Faculty members may provide much expertise, but due to the volume of technology out there and its short half-life, instructors will not routinely be able to have expertise in all of these hands on areas. Effective laboratory operation demands a dedicated administrator.

7. Conclusion

In this paper we have described the requirements for a comprehensive computer and network forensics training and education program. We partitioned the forensics discipline into the four categories of Evidence Collection, Evidence Preservation, Evidence Presentation, and Forensic Preparation, and proposed four levels of CNF positions.

We gave an overview of the subjects that may be taught in academic CNF programs and asked which broader academic concepts might need review. We then offered suggestions about how such a program can fit into the academic environment and gave two case studies, one of a CNF class in an Information Technology department. In the second case study, we explained how matters had developed in the United Kingdom. We concluded by describing the challenges relating to establishing a CNF laboratory.

With the explosive growth of the Internet and corresponding increase in computer related crime, it is essential and inevitable that CNF training and education programs will appear. It is our hope and intention that these programs will not be developed in a vacuum or without thought of how best to form a global CNF workforce.

8. Bibliography

[1] Sommer, Peter, “Intrusion Detection Systems as Evidence”, *Computer Networks, Volume 31, Issues 23-24, 14 December 1999, Pages 2477-2487*

[2] Center for Secure and Dependable Software (CSDS) Forensics Workshop, University of Idaho, September 23-25, 2002

[3] National Security Agency, National INFOSEC Education & Training Program (NIETP), Centers of Academic Excellence in Information Assurance Education Program, http://www.nsa.gov/isso/programs/coeiae/index.htm

[4] Yanet Manzano and Alec Yasinsac, "Policies to Enhance Computer and Network Forensics", The 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, held at the United States Military Academy, June 2001