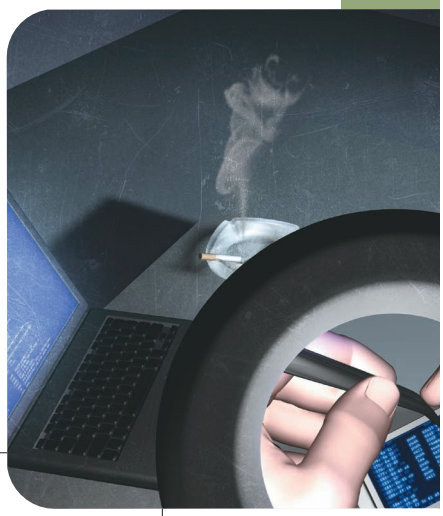
Computer Forensics Education

The application of science and education to computer-related crime forensics is still largely limited to law enforcement organizations. Building a suitable workforce development program could support the rapidly growing field of computer and network forensics.



Alec Yasinsac
Florida State University

Robert F. Erbacher
Utah State University

Donald G. Marks
Central Michigan University

Mark M. Pollitt
US Federal Bureau of Investigation

Peter M. Sommer
LSE Computer Security Research Centre

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.

A key step in improving forensic techniques lies in creating a comprehensive approach to forensics education. However, the efforts of theorists and practitioners in this new field have yet to converge to the point of producing a usable pedagogical model. The academic community, for example, appears immersed in counterhacking technology, which stems largely from intrusion detection and survivability research. Conversely, the demand for computer forensic techniques (to recover data and attribute its origin to perpetrators and victims) drives practitioners in the judiciary field.

As an attempt to close this theory–practice gap, we propose some generic requirements, resources, and pedagogical approaches for developing and implementing a forensics program in higher education. We don't expect our results to be implemented directly, but we do intend them to stimulate thoughtful discussion, as did the workshop at which many of these ideas originated (the Center for Secure and Dependable Software Forensics Workshop held at the University of Idaho, 23–25 September 2002).

Evolution

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*.[1]

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.

In this article, we describe analytically valuable data in both its dynamic (network traffic) and static states (media). Although network traffic often is relevant to intrusions, we need media analysis to investigate the crime's conventional aspects. Suppose, for example, that a suspect eludes police but abandons a laptop computer. 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 impor-

tant 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. Moreover, the fledgling field developed apart from the mainstream of forensic science—without the benefits of peer-reviewed journals and standard operating practices.

The computer security community traditionally has focused on protecting information systems from attack, with forensic techniques used peripherally in the intrusion detection community.[2,3] 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.[4] Soon, various communities wanted the process to be canonized to let practitioners repeat successes and avoid flawed or less productive methods. Localized—but fragmented—ad hoc training programs started appearing out of necessity. 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). Still, little foundational work is published anywhere, although we used similar work in the computer and network security area[5–9] as a springboard to observations and recommendations.

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.

A computer forensics case study

Let's look at a real-world scenario and how computer forensics plays into it. Late one night, a system administrator (sysadmin) 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 sysadmin, 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. But there's a far better way to handle this situation.

The boss instructs the sysadmin 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 sysadmin'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 workstation. 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. On the basis of 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,[10]
- Industry needs professionals with computer forensic competence as well as specialized computer forensics technicians, and
- 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. Our view of these positions was influenced in part by the US National Security Agency's information assurance workforce development programs.

CNF technician

The CNF technician position is where the forensics rubber meets the road. People in this position exercise the technical aspects of gathering evidence, so 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.

A CNF technician can get by with an associate's degree from a two-year college, but a four-year degree with an emphasis on technology is the most advantageous career choice. It might even be a requirement for anyone wishing to be promoted to CNF professional.

CNF policy maker

At the other end of the forensics spectrum is the CNF policy maker. This type of manager or administrator establishes CNF policies that reflect the enterprise's broad considerations. It is the policy maker's responsibility to see the impact of forensics in the broader context of business goals and make the hard decisions that trade off forensics capabilities with issues of privacy and, correspondingly, morale.

Although 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.

CNF professional

Although the CNF technician performs 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 a broad and deep understanding of the legal procedures and requirements gained through either a broader education or extensive experience. Moreover, the CNF professional must understand the fundamental enterprise business to ensure that CNF policies are executed properly within the business context.

CNF researcher

Although CNF is not yet fully recognized as an independent discipline, it has clearly surpassed the development status it held in the early Internet years. Moreover, there is a demand for educators who specialize in it. Although CNF professionals might be able to double as trainers for elementary computer and evidence discovery classes, graduate degrees are required to introduce these courses into higher education.

As with its sister discipline (computer and network security), 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. Academia will employ most CNF researchers, although a few will be needed in large federal and state government agencies. Career progression into the CNF policy maker is a possibility in certain instances.

Forensics curriculum

Computer forensics is multidisciplinary by nature, due to its foundation in two otherwise technologically separate fields (computing and law). Several other fields are also involved, mostly related to criminology, information sciences, and computer engineering. To structure the topics in this field, we can partition them into four categories: evidence collection, evidence preservation, evidence presentation, and forensic preparation. These categories support, but are orthogonal to, the CNF positions just described (see Table 1).

Table 1. Computing forensics skills distribution.

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 2. Training versus education.

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

Evidence collection

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

In CNF, simply knowing where to look frequently uncovers information. Forensic investigators can find information hidden in logs, caches, swap files, deleted files, or 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 forensics expert's unique responsibility to know the myriad nooks and crannies where important tips and evidence can hide.

Data recovery, on the other hand, is the result of applying extraordinary measures to extract information from locations in which it is known to reside. The best-known illustration of data recovery is recovering information from electromagnetically wiped or damaged disk drives.[11] 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 partitioned into packets must be reconstructed into sessions to recover relevant information. Discovering and recovering information is the heart of computer forensics.

Evidence preservation

Once information is recovered, rigid requirements help preserve it for later use in court. Preservation helps CNF experts answer two important questions: Was the evidence gathered properly, so that it reflects all the pertinent information on the subject device when it was collected? Has the evidence been changed since it was collected?

Technology such as secure copying and storage mirroring provide mechanisms for showing the acquired evidence's accuracy. Mirroring simply means making an exact copy of an entire storage device; the CNF expert can extract relevant information from the copy without disturbing the original device. Secure copying techniques let investigators bind the target information to some other information that verifies the copy's accuracy.

Cryptographic digital signatures, in conjunction with strong physical security, provide the potential to protect digital evidence's integrity even further. With proper preparation and tools, these signatures can be made tamper-resistant against even the most sophisticated intruders and can be reconstructed from the presented evidence to ensure authenticity.

Evidence presentation

Digital evidence is notoriously difficult to present in court, the greatest challenge being that it has no natural physical character: digital evidence is essentially abstract. To further complicate this challenge, although computers are pervasive in society, most people in the juror pool have little understanding and possibly little exposure to computers, networks, and digital information.

When introducing digital evidence, presenters should put themselves in the juror's place by studying case histories and using simple and sophisticated graphics to make a digital case. Unfortunately, though, few computer technicians or experts are familiar enough with the difficulties in presenting evidence in court or with the mechanisms that can facilitate the process. A comprehensive CNF program should include instruction in theory and methods of effectively presenting digital evidence in court.

Forensic preparation

Forensics efforts traditionally start after a malicious act occurs. As the CNF field evolved, Yanet Manzano and Alec Yasinsac recognized[12] that much could be done to facilitate forensics investigation before malicious acts happen. In much the way that surveillance cameras help make the case against shoplifters, electronic mirroring, logging, and marking help investigators reconstruct malicious acts

Table 3. Computing forensics training plan.

ROLE	EDUCATION	TRAINING
CNF technician	Introduction to forensic science Introduction to computer science Introduction to computer hardware Introduction to operating systems Introduction to criminal and civil law	A+ training Net+ training Basic computer seizure Basic data recovery and duplication
CNF policy maker	Information management Forensic science Information assurance Knowledge management Enterprise architecture	Survey or seminar courses in information assurance, legal issues, and CNF techniques
CNF professional	All of CNF technician items Upper-level BS/MS courses in information systems,network systems, architecture, and criminal, civil, and procedural law	All of CNF technician training plus advanced data recovery and moot court training
CNF researcher	Doctorate-level education or a masters degree with extensive experience in computer forensics	Specific research areas are difficult to project, but researchers should receive hands-on training in the research areas

and trace attackers. Watermarking technology (inserting marks that identify stolen information after it is discovered) also continues to evolve.

Forensic preparation techniques present an opportunity for instructors to bring a strong research component into the classroom when presenting these topics.

Education and training

A comprehensive CNF curriculum must include a variety of topics, many of which are clearly educational and reflect an appropriate level of academic abstraction. However, many topics are skills oriented and better suited to a training program. The computer security field crosses both the training and the 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 up to the doctoral level. A similar structure is appropriate for a comprehensive CNF workforce (see Table 2).

We can best illustrate the distinction between training and education 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, others emphasize report-writing skills, and still others provide strong artificial intelligence and data-mining features. Although it is important to understand the investigative procedure, it is not essential that technicians understand the tools' internal operations. The emphasis in not on tool detail but what the tool reveals about the data and its underlying structure.

Conversely, tool builders must have a 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 tools' input and output as well as the way the technicians expect to use them. This description fits CNF researchers and some CNF professionals. Adequate preparation for this career path will require a strong, traditional computer science background, especially with programming skills (see Table 3). The CNF technician, policy maker, and professional are well served by courses commonly offered as part of an IT degree. A few traditional computer science courses also would be appropriate—certainly in architecture, assembly language, comparative operating systems, and networking.

Undergraduate education

Computer forensics is well suited to undergraduate classes. Although outstanding research questions abound in the field, a large body of expertise, techniques, and knowledge can be presented to undergraduates. Analyzing all the data on a hard disk, for example, requires a detailed knowledge of the operating system. Moreover, students must know where to look for email archives, how Internet queries are stored in the system, how to reconstruct evidence from partially overwritten files, and other activities. The reconstruction of user activity from data artifacts in permanent storage is a great learning experience for budding computer scientists, and it solidifies lessons learned in many other classes.

One objective of undergraduate education is to prepare graduates for employment. As the criminal element in society learns to use computers for personal and professional activities, police departments at all levels will most likely increase their hiring of computer forensic experts. Similarly, the legal defense community (both lawyers and expert witnesses) will need to expand its base of expertise to defend clients. Although the number of computer forensics experts might not be large, the students who craft a course of study aimed at becoming a CNF expert will find ample employment opportunities.

Undergraduate programs can provide an ideal venue for training forensic technicians with the technical skills to discover and preserve CNF evidence. The programs also provide a closely related program that gives forensic professionals the breadth and multidisciplinary information needed to oversee CNF programs. Computer forensics also provides training for system administrators who might have to investigate employee use of company computers. Although this is an administrative (not a criminal) offense, data examination requires the same technical expertise.

Computer forensics classes must cover an in-depth analysis of several software systems including operating systems, email 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 tricks. This decomposition of software packages aids their understanding of how large projects are built, how individual programs interface with the operating system and other applications, and how to analyze data independently of the application that uses or creates that data.

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 construct helpful tools on the fly. Table 3 illustrates how these positional models might intersect with existing and future courses.

Finding a home for an academic CNF program

Because of its multidisciplinary character, a computer forensics course's best fit in a university is unclear. Its placement is further complicated by the rapid growth and focus of computing-related disciplines and departments in universities. In addition to ubiquitous computer science departments, 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, and so on. All these departments inform a backdrop suitable for providing the computer-related training essential to a CNF curriculum. For ease of reference, we refer to this group of departments as *computing sciences*.

Several other departments in academic colleges and universities argue that their criminology or criminal justice departments are best suited for a CNF program because forensics of any type is just a law enforcement tool. Unfortunately, criminology and criminal justice departments usually don't have the expertise or resources to offer a computer-based course any more than they have the means to open their own medical schools to prepare forensic doctors. Conventional forensics courses are frequently taught in university chemistry and physics departments, so there is no additional reason to handle computer forensics in the criminology department.

One feature that distinguishes computer forensics from other branches of forensic science is the rate at which new hardware platforms, operating systems, integrated environments, applications, and so on, appear, and how this boom produces cultural changes in the way in which people use computers. Even in the last two years, we have seen considerable growth in the use of peer-to-peer infrastructures. These technological changes happen more rapidly than the steady process of peer-reviewed articles and syllabus development allow.

A further important conceptual issue is how far to take individual forensic examinations. In most real-life situations, forensic resources are limited, so their deployment must produce results. How do we balance this against a computer engineer's natural tendency to be unsatisfied with anything less than the most thorough result possible?

Finally, computer engineering 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. Computer engineering is an essential component of a CNF program, though, so forensics applications should represent only a narrow range of a computer engineering department's scope.

Thus far, our discussion of selecting the proper department for a computing forensics program has raised more questions than answers. Let's look at two case studies of such programs in dramatically different environments. The first describes a forensics education program established in an information technology department, while the latter was established in a military science department and geared toward law enforcement and military activities.

Case study I: Central Michigan University

Courses in computer forensics are not widely offered in academia, so the decision to offer such a class at Central Michigan University offered unique insights into the

interest, requirements, and difficulties of starting up such a program.

The class garnered a lot of student interest: in the wake of 9/11, there was a palpable hunger to contribute something to the war on terrorism. The course had 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 studying various cryptography implementations but then expanding to study steganography, theoretical cryptography, and specialized forensic hardware. The students usually met in the evenings, but some decided to meet on Saturday mornings—a bit unusual considering it was in addition to their full load of studies.

This enthusiasm was not limited to the students—the school 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 (which initiated a new computer-disposal policy), and the library became increasingly aware of computer security and forensics. Input from these various interest groups should not be overlooked. Each group or department contributed its 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.

Unfortunately, some problems surfaced in the forensics class. The course requires several hands-on case studies to be available for the students, and each student, or small group of students, must have root access to an individual machine to perform network forensics. Similarly, the commercial media analysis programs were not network capable, so individual copies of that software were required (a very expensive proposition). If other classes shared the computer laboratory, setup and teardown operations for each experiment were labor intensive and required several personnel to assist the instructor. To avoid such problems, a laboratory devoted to computer forensics should suffice. Similarly, a single computer for independent study is a good choice. Setting up a general-purpose laboratory for several other classes is difficult and requires considerable planning.

Case study II: Experience in the United Kingdom

Detectives in the UK discovered computer crime and forensic computing quite early; they set up a Computer Crime Unit (CCU) within Scotland Yard in 1985. Today, the UK's lead law enforcement body is the National High Tech Crime Unit, which 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 at Interpol. These courses emphasized practicality and were orientated toward disk forensics.

Other police forces and law enforcement agencies set up their own training schemes, but there was little coordination. Eventually, an informal group of law enforcement officers became subsumed in a Digital Evidence Group run by the Home Office. In the mid-1990s, the Royal College of Military Science at Shrivenham established a set of "short" courses on computing forensics. These courses were geared toward law enforcement, the military, and the security service, and they tended to concentrate on the discipline's computer science and hardware aspects.

Following a national reorganization of the UK police in 1997, Shrivenham continues to provide high-end academic training for law enforcement—an MSc course began in 2002. The more vocational forms of training are available from a new specialist center, which provides courses in network investigation, disk forensics, and computer forensics for line managers and child abuse specialists. Training from product vendors is also available, although law enforcement agencies are always anxious to avoid becoming overly dependent on any one product. Training for non-law enforcement personnel is difficult to obtain, but the authorities are willing to involve defense experts in their deliberations. In the UK, the duty of an expert hired by the defense is to the court, not to the defendant.

An academic forensic laboratory

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

Laboratory spaces

Much of a CNF program's hands-on work can be accomplished in existing departmental laboratories. In fact, many of the forensics tools can use the variety of activity recorded on public machines to their advantage.

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

Table 4. Devices for use in a CNF laboratory.

COMPUTERS		NETWORK	SECURITY	PERIPHERALS	OPERATING SYSTEMS	APPLICATIONS	CNF TOOLS
Workstations	Intel	Routers	Firewalls	Disk drives	Unix	Office suites	SNORT
		RISC	Switches	Intrusion detection	Disk recovery equipment	Solaris	Middleware
Macintosh	Proxies		Printers	Windows			
Servers	Intel			CD recovery	Linux		
RISC				Macintosh			

Equipment for a CNF laboratory

Because many CNF projects are similar to other computing sciences projects, students can conduct them on existing departmental resources, if sufficient laboratory space is available. However, a new CNF program will increase the demand and usage of the introducing department's public computers.

Some CNF projects are not suitable for public laboratories and thus require a dedicated and segregated CNF network. The Internet is a highly heterogeneous environment, so a CNF laboratory should have a variety of equipment for workstations, peripherals, and network equipment. Workstations should be available in the three most popular operating systems (Unix, Windows, and Macintosh); network equipment should include hubs, switches, routers, firewalls, proxies, and other devices that can store information useful in an investigation (see Table 4). To allow flexibility in experimentation, these devices should not be integral components for the laboratory's connectivity.

Software to support a CNF laboratory

As Table 4 shows, three categories of software are necessary for a CNF laboratory: tools, user operating systems, and user applications. The tools should be available to students for evidence discovery and recovery, the operating system software helps emulate perpetrator and victim machines, and the applications can emulate victim information and processes.

Much of this software is available as freeware; you can also attain it as shareware or as a demo copy for project purposes. On the proprietary side, vendors might 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.

CNF laboratory support personnel

The final resource a CNF laboratory needs is support personnel. Leveraging existing technical support staff to operate and maintain new laboratories is financially appealing, but they are likely already overtaxed and don't 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 have expertise in all these hands-on areas. Effective laboratory operation demands a dedicated administrator.

With the Internet's growth and the 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.

The opportunity is great. Like television, computing has permeated society very quickly and with a dramatic impact. Unlike television, though, computing technology is a prime target and tool for criminals because of its interactive nature, ability to store important information, and use in commerce.

Presently, computing forensics training is provided almost exclusively by law enforcement organizations; only a few universities support computing forensics programs, and most comprise only one course. We expect this to change over the next three to five years, and we hope that evolving programs can leverage experience gained through the recent US National Security Agency-prompted expansion of information-assurance education programs. The health of the Internet itself may depend on it. □

References

1. P. Sommer, "Intrusion Detection Systems as Evidence," *Computer Networks*, vol. 31, nos. 23–24, 1999, pp. 2477–2487.
2. K. Rosenblatt, *High Technology Crime*, KSK Publications, 1995.
3. D. Icove, K. Seger, and S. VonStorch, *Computer Crime: A Crimefighter's Handbook*, O'Reilly & Associates, 1995.
4. R. McKemmish, "What Is Forensic Computing," *Trends and Issues in Crime and Criminal Justice*, no. 118, Australian Inst. of Criminology; www.aic.gov.au/publications/tandi/index3.html.
5. C.E. Irvine, S.-K. Chin, and D.A. Frincke, "Integrating Security into the Curriculum," *Computer*, vol. 31, no.

12, 1998, pp. 25–30.
6. C.E. Irvine, "Amplifying Security Education in the Laboratory," *Proc. 1st World Conf. Information Security Education* (IFIP TCII WC 11.8), 1999, pp. 139–146.
7. A. Yasinsac, "Information Security Curricula in Computer Science Departments: Theory and Practice," *5th Nat'l Colloquium Information Systems Security Education 2001: A Security Odyssey*, NCISSE Colloquium Press, 2001.
8. A. Yasinsac, J. Frazier, and M. Bogdonav, "Developing an Academic Security Laboratory," *Proc. 6th Nat'l Colloquium Information Systems Security Education*, NCISSE Colloquium Press, 2002.
9. J.E. Anderson and P.H. Schwager, "Security in the Information Systems Curriculum: Identification & Status of Relevant Issues," *J. Computer Information Systems*, vol. 32, no. 3, 2002, pp. 16–24.
10. G. Shpantzer and T. Ipsen, "Law Enforcement Challenges in Digital Forensics," *Proc. 6th Nat'l Colloquium Information Systems Security Education*, NCISSE Colloquium Press, 2002.
11. S.L. Garfinkel and A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practices," *IEEE Security & Privacy*, vol. 1, no. 1, 2003, pp. 17–27.
12. Y. Manzano and A. Yasinsac, "Policies to Enhance Computer and Network Forensics," *Proc. 2nd Ann. IEEE Systems, Man, and Cybernetics Information Assurance Workshop*, IEEE CS Press, 2001, pp. 289–295.

Alec Yasinsac *is an assistant professor of computer science at Florida State University. His research interests include network security, computing forensics, and formal methods. He received his PhD in computer science from the University of Virginia. He is a senior member of the IEEE. Contact him at the Computer Science Dept., Florida State Univ., Tallahassee, FL 32306-4530; yasinsac@ieee.org.*

Robert F. Erbacher *is an assistant professor in the Computer Science Department at Utah State University. His research interests include computer graphics, information and scientific visualization, and computer security. He received his SCD in computer science from the University of Massachusetts, Lowell. Contact him at the Dept. of Computer Science, Utah State Univ., 4205 Old Main Dr., Logan, UT 84322-4205; Robert.Erbacher@usu.edu.*

Donald G. Marks *is an associate professor at Central Michigan University, but is moving to an equivalent position at the University of Tulsa in Fall 2003. He has served on many US government initiatives, including Critical Infrastructure Protection, the Research Council, the Network Security Information Exchange, and several academic funding initiatives. He received his PhD in information technology from George Mason University. Contact him at the Dept. of Mathematical and Computer Sciences, Univ. of Tulsa, Tulsa, OK 74104; donald-marks@utulsa.edu.*

Mark M. Pollitt *is a 20-year veteran of the US Federal Bureau of Investigation, where he is director of the FBI's Regional Computer Forensic Laboratory Program. He received his MS in information management from Syracuse University. Contact him at mark@digitalevidencepro.com.*

Peter M. Sommer *is a senior research fellow at the Computer Security Research Centre in the London School of Economics. He is an external examiner for the Forensic Computing MSc at the Royal Military College of Science, advises on police high-tech crime education, provides training for the Crown Prosecution Service, and has acted as expert in many important computer crime trials. Contact him at the London School of Economics and Political Science, Houghton St., London WC2 2AE, United Kingdom; p.m.sommer@lse.ac.uk.*