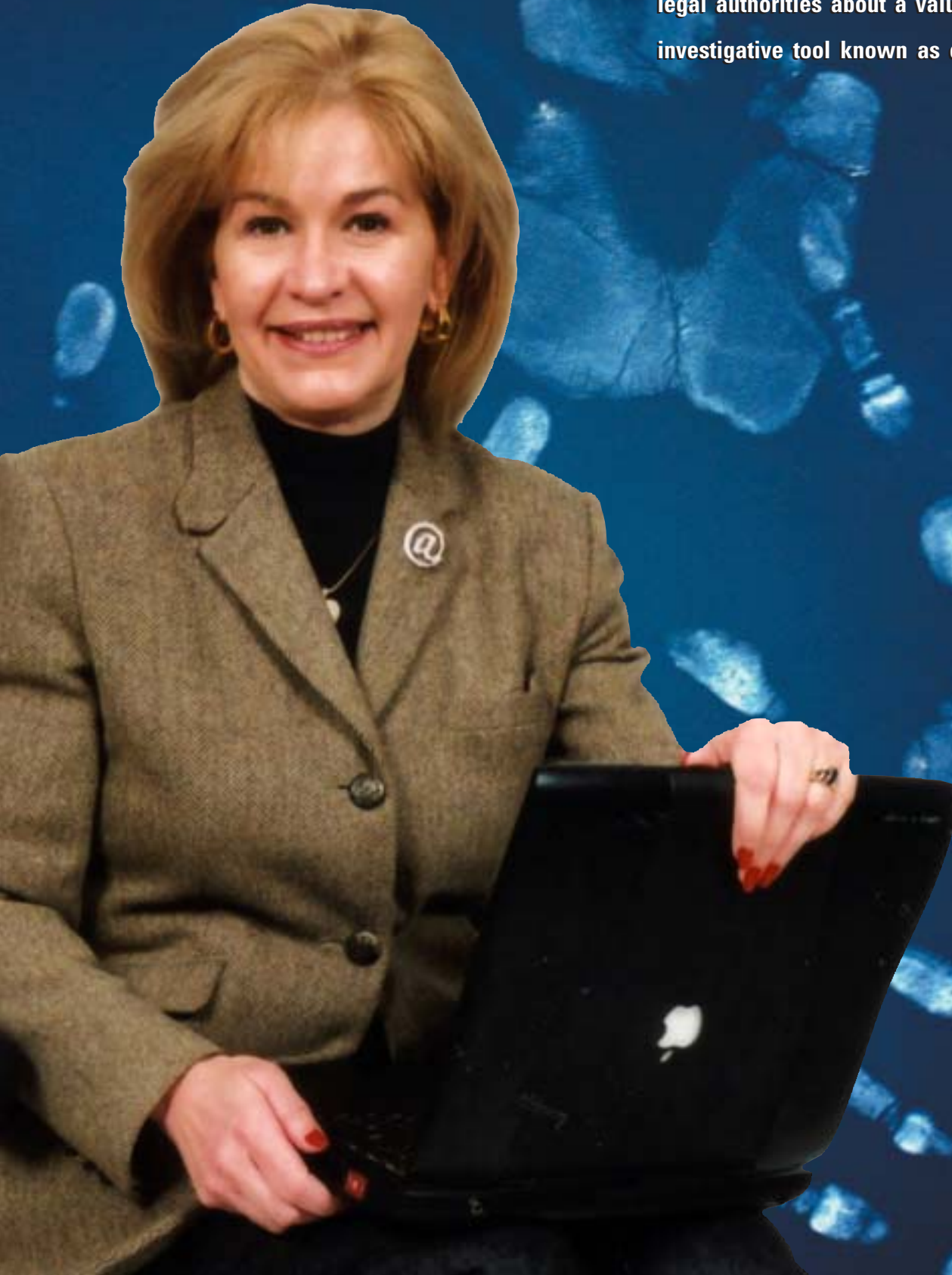


Combating Computer Crime

Dr. Linda Volonino educates law enforcement and legal authorities about a valuable new criminal investigative tool known as computer forensics



WHEN FEDERAL AUTHORITIES

arrested self-proclaimed September 11 mastermind, Khalid Sheikh Mohammad, in March, a team of cyber investigators sifted through the thousands of documents and E-mail correspondence found in the computers confiscated from his Pakistan home.

When bankrupt energy giant Enron and its auditor, Arthur Andersen, shredded thousands of evidential documents, the PC police were called in to track the digital trail left behind on the companies' E-mail servers, laptop and desktop computers. And in 2001, when a 15-year old Connecticut boy hacked into a government computer system that monitored positions of U.S. Air Force planes, federal computer forces tracked the intrusions back to the teenager's home.

In all these cases, authorities were able to uncover the cyber trail that others thought had been destroyed, using computer forensics – a new investigative tool employed by law enforcement.

"Forensics is simply the discovery of evidence. In a murder case, it could be fingerprints," explains Dr. Linda A. Volonino, chair of information systems (IS) and director of telecommunications at Canisius College. "In the digital world, it's where you went on the computer, what Web sites you visited and what files you opened or E-mailed."

Unlike fingerprints, however, which can be wiped clean, forensic evidence of the electronic kind may be permanently stored in hard drives, on server networks and backup servers, as well as on laptop computers, cellular phones, fax machines and personal digital assistants (ex. Palm Pilots).

"There are now electronic trails where there weren't before," states Volonino, who uses E-mail as an example. "It's almost impossible to permanently delete or destroy E-mails simply because whatever path the E-mail took can be traced back to the servers that were hit along the way, such as AOL or Netscape. People just don't realize there are backup copies of virtually everything they do and everywhere they go on the computer."

As a result, those trained to track digital data will almost always find a trail. And with computer crimes increasing in both frequency and destructive power, law enforcement and

legal authorities are turning to computer forensic savvy people, such as Volonino, to help contend with the technical issues. Considered among the top professionals in the growing field of computer forensics, Volonino's interest in the subject dates back to 1998 when she was asked to speak "on a unique computer topic," at a two-day continuing education class. In searching the Internet for ideas, she came across the subject of computer forensics.

"I thought it was a great topic because at that time, no one was really aware of just how much information they were giving away about themselves through the computer, or the ways in which company information and integrity could be jeopardized." She adds that crimes committed via the computer (such as identity theft, extortion, money laundering or pornography) can be hidden within Word, Powerpoint or Excel documents and then E-mailed out as attachments. Volonino notes, "Excel spread sheets are a major conduit for transmitting pornographic images and no one ever thinks to look there."

As one of the few people in on the ground floor of computer forensics, Volonino's extensive knowledge on the subject makes her someone people turn to, to learn more about this growing field. At Canisius, that resulted in her establishing cyber security and computer forensic courses, at the graduate and undergraduate level. These courses are now giving students and the college a cutting-edge advantage in the IS field. Volonino also volunteers much of her time and computer know-how to educate the public at-large, through what she refers to as an academic-government alliance.

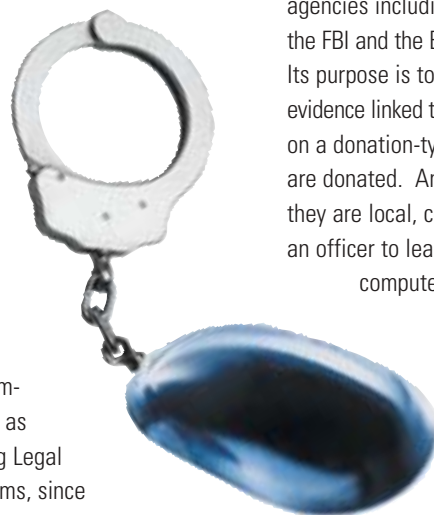
Local law enforcement agents and lawyers keep Volonino particularly busy, as they try to learn computer language and technology well enough to explain to a jury. Several law firms recruit her to teach computer forensic classes, as part of their Continuing Legal Education (CLE) programs, since

"lawyers are only interested in evidence." Those same firms also call on Volonino to testify as an expert witness in computer crime cases. Most recently, the name of this Canisius College professor came to the attention of Michael Battle, U.S. Attorney for the Western District of New York, who needed a crash course in computer forensics.

"A year ago, I could not have had this conversation because I did not have an understanding about the importance of computer forensics nor did I understand the need," says Battle. He notes that in traditional law enforcement, authorities executing a search warrant in a suspected drug house might find residue, scales or other accretions of the drug trade. Contrary to tradition, however, today's criminal activity is being stored and committed on computers. As a result, Battle says authorities are now having to learn how to seize and preserve computers, so as not to compromise evidence. He adds, "If we had to pay for Linda's type of expertise or go outside the community to get it, it would be very expensive and very time consuming. She is a valuable asset in terms of providing education to our law enforcement people and in helping me educate the government, on the local and national level, on how to go about utilizing this very valuable criminal justice tool."

Last summer, Battle enlisted the expertise of Volonino for a proposal he planned to present to U.S. Attorney General John Ashcroft, aimed at securing federal funds for the Regional Computer Forensics Laboratory in Cheektowaga. The lab was opened with the combined resources of numerous local, state and federal agencies including the U.S. Attorney's Office, the FBI and the Erie County Sheriff's Department. Its purpose is to investigate and analyze digital evidence linked to computer crimes but it operates on a donation-type basis. Equipment and space are donated. And the police agencies, whether they are local, county sheriff or FBI, each donate an officer to learn and work in the computer forensics lab, for a designated period of time.

"Mike's thought was 'enough of this relying on donations and volunteers for something so important,'" explains



Volonino. "He wanted a federally funded computer forensics lab. To do this of course, it has to go through John Ashcroft. So he asked for my feedback on a proposal he was writing about why we needed this lab to be federally funded."

As Battle awaits word of approval on the proposal, which he presented in fall 2002, Volonino continues to assist the U.S. Attorney's Office in combating computer crime, which has become a primary challenge for 21st century law enforcement.

"The advent of the computer gave every traditional crime a new playground in which to be conducted," says Volonino. Not surprisingly, this new playground has resulted in a rapid rise of computer-mediated crimes and crimes against computer network systems.

Of the 625 million Web users, worldwide, in 2002, there were approximately one million criminal and civil complaints filed to authorities. The most popular targets of cyber attacks are U.S. corporations and organizations, which can financially bleed as a result of computer break-ins. Just last year, about \$5 billion worth of software was stolen over the Internet. Telephone companies suffered a \$1 billion loss from phone card numbers stolen via the computer. Credit card corporations reported an estimated \$3 billion in losses due to computer theft. All in all, the research division of InterGOV International estimates that cyber terrorism took a \$50 billion toll on corporations and organizations in 2002.

"Cyber terrorism essentially deals with a computer attack on a critical infrastructure via the Internet," explains Volonino. "An attack on a telecommunications industry would be one example. An attack on a financial network would be another."

But unlike hackers, who do not typically intend to cause disruption, cyber terrorists are "people who either want to steal, alter or remove data, or disrupt the communications system in an attempt to cause chaos and impede the ability of communications or financial networks," says Assistant U.S. Attorney Martin L. Littlefield, who specializes in prosecuting computer crimes.

There are ways to safeguard against cyber terrorism, however, and so last April, when Littlefield was assigned the task of organizing a cyber terrorism seminar for the Western New

York business and educational community, and local, state and federal law enforcement, he recruited Volonino to serve as one of the guest speakers.

"When I'm called in on a computer forensics case it's because something has already gone wrong," states Volonino. "The seminar gave

"Linda is a consummate, well-respected, renowned professional and the kind of go-to person that the business and legal community looks to for assistance."

— MARTIN LITTLEFIELD, Assistant U.S. Attorney

me the opportunity to help educate law enforcement, corporations and organizations about precautions and safeguards that can be taken to prevent things from going wrong."

Volonino spoke to an audience of 225 people about the common vulnerabilities found in computer networks and advised them on preventative measures to protect their businesses or organizations from a cyber attack. It wasn't her first such talk on the topic. Volonino has traveled to the United Arab Emirates in the Middle East to speak at the Etisalat Academy (telecommunications university) about possible cyber terrorism threats and preventative measures. She has also addressed the Canadian Internal Revenue Service and Customs Agency on similar topics. And as a member of the FBI's InfraGard, Volonino frequently interacts with various community and corporate leaders to warn of potential cyber targets and security steps.

"The goal of the InfraGard is to create an industry-government alliance in which the FBI and corporate community can share information about potential problems or cyber threats," explains Volonino.

Made up of FBI agents and information technology people from banks, insurance companies, law firms and colleges, there are nearly 60 InfraGard units nationwide. Once under the direction of the FBI, the agency now operates under the new Department of Homeland Security and members of each local unit meet quarterly to discuss the latest cyber threats to critical infrastructure, cyber exploits, vulnerabili-



Dr. Linda Volonino's working relationship with the U.S. Attorney's Office is also helping to educate Canisius students. In March, Assistant U.S. Attorney Martin L. Littlefield served as a guest speaker in her telecommunications seminar course. Littlefield spoke about federal legislation regarding computer crime.

ties and countermeasures.

"As a member, I get National Infrastructure Protection Reports, or warnings, everyday," explains Volonino. "I receive warnings for information technology. There are warning reports for the banking industry. At our meetings then, we make sure everyone knows what is going on and what threats are out there."

With education being the key to cyber security, Volonino is committed for the long haul to teach the tools of the trade. She says, "Knowing what's at risk, I want to work for the side that's taking protections and precautions."

That is encouraging news for people like Martin Littlefield and Michael Battle who say the U.S. Attorney's Office will continue to engage the expertise of Volonino to educate law enforcement on how to keep pace with and track of today's high-tech criminals.

"Linda is a consummate, well-respected, renowned professional and the kind of go-to person that the business and legal community looks to for assistance," says Littlefield. "She's been helpful to me. She's been helpful to the lawyers in this office. And she's been helpful to law enforcement in our efforts to educate the community about the kinds of efforts we're putting forth to improve our ability to examine evidence of crimes that utilize computers," says Battle. "I fully expect to call on her in the future." ■