Cyber Forensics and the Changing Face of Investigating Criminal Behavior

By Kent Mortimore, Al Marcella Jr., and Doug Menendez – ISSA member, St. Louis, USA chapter

The emergence of new technology requires the law enforcement community – from police to prosecutors to judges – to utilize different strategies and different tools in addressing the new ways today's criminals commit old crimes.

Identity theft, a term almost unheard of 30 years ago, now makes up significant portions of the case loads of police agencies and prosecutors in the United States.[1] The problem has become so pervasive that specific statutes designed to address the problem have been enacted in numerous jurisdictions including under federal law. See, e.g., Identity Theft and Assumption Deterrence Act, Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998).[2]

In reality these identity theft cases present very little that is actually new in the realm of criminal behavior. But the emergence of new technology requires the law enforcement community – from police to prosecutors to judges – to utilize different strategies and different tools in addressing the new ways today's criminals commit these old crimes.

In addition to identity theft, the computer and the Internet allow malicious cybercriminals to violate copyright protection, cause enormous damage to data and equipment, and to lure children and even adults into situations where they can be sexually and physically assaulted.

New technology provides opportunities for criminals in many areas. Police now frequently chronicle criminals' use of the Internet and computer technology to commit a wide range of economic crimes and crimes involving malicious destruction of others' property.

1 United States Department of Justice. Bureau of Justice Statistics 2006. Identity Theft from www.ojp.usdoj.gov/bjs/abstract/it04.htm.

2 http://www.ftc.gov/os/statutes/itada/itadact.htm.

Evidence in the 21st century

Traditional evidence in criminal cases has substance, shape, and form. People can see it. In many cases they can touch it. Fingerprints, for example, are often visible on surfaces like table tops. Even where they are latent, simple techniques exist for their retrieval. And fingerprints can last for years or even decades under the right conditions, as can trace evidence like hair and fibers. Computer evidence is entirely different. It cannot be seen, touched, or smelled, and it often lasts for only very short periods of time.

Computers typically store data in three ways, magnetic, semiconductor, and optical. Other less common data storage methods include magneto-optical disk storage, optical jukebox storage, and ultra-density optical disk storage.

Data stored on these devices, while potentially of tremendous value in the investigation, prosecution, and prevention of crime, presents unique challenges to detectives and prosecutors because of its potentially volatile nature. Electronic data is fragile. It can easily be changed or eliminated. Thieves and other cybercriminals, along with dishonest and even honest employees, can easily change the nature of this information – often unintentionally. Cyber forensics is the process of finding, extracting, preserving, and understanding electronic data while providing a guarantee that the data was not altered during the investigation.

Cybercrime defined

Cybercrime is typically described as any criminal act dealing with computers or computer networks. It is also called by other names (eCrime, computer crime, or Internet crime in different jurisdictions) which have roughly the equivalent meanings. In most cases cybercrime is a general – as opposed to a legal – term, although some jurisdictions have provided specific definitions for cybercrime behavior (e.g., Oregon Revised Statutes 164.377[3]). Other jurisdictions take a somewhat more expansive approach by not trying to assign a specific definition, but rather by trying to address criminal behavior in the context of the use of computers.[4]

Regardless of the definitions, the use of computers and the Internet in the commission of crimes requires investigators applying cyber forensics techniques to extract data for those investigating these cases, prosecuting these cases, and passing the ultimate judgment regarding the disposition of offenders and the redress of victims.

Economic aspects of cyber forensics

The increasing globalization of the world's economy and infrastructure has dramatically influenced the logistics of criminal investigations at both local and international levels. With worldwide availability of the Internet, and with English language skills now taught in schools throughout the world, criminals no longer need to be physically present in a community or even a nation in order to violate the laws there. In fact, these perpetrators can identify targets, carry out their schemes, and withdraw with all of the benefits of their illegal activities from literally any place on the globe with Internet connections. Their targets can reside in places where the criminals have never visited.

This reality prompted the U.S. Federal Bureau of Investigation (FBI) to make cybersecurity the third prong of its mission. Director Robert S. Mueller noted:

> The globalization of crime – whether terrorism, international trafficking of drugs, contraband, and people, or cybercrime – absolutely requires us to integrate law enforcement efforts around the world. And that means having our agents working directly with their counterparts overseas.[5]

The magnitude of the problem cannot be understated. The FBI estimates that in the course of one year as many as 10 million Americans are the victims of identity theft alone.[6] Cybercrime is increasing at a disproportionate rate as compared to more traditional crime.

Practical issues

In both traditional and non-traditional investigations, detectives must have access to relevant evidence and to witnesses. They photograph and seize physical evidence. They create maps and diagrams of crime scenes. They document victims' injuries or economic losses. They interview witnesses and suspects. All of these components of a thorough investigation are required for a successful prosecution. Under the Fourth and Fourteenth Amendments to the U.S. Constitution, criminal suspects are afforded all the guarantees of due process, including most importantly the presumption of innocence. Without sufficient proof, no conviction can be sustained. But cybercrimes present new challenges and tasks that change the tactics and economics of criminal investigations.

Any such investigation first begs the question of cost. While the traditional criminal investigation requires a detective or police officer to drive or walk to the scene of the crime to seize evidence and interview the principles, the typical cybercrime can require air travel, great expenditures of time, and confusing rules regarding both the logistics and legalities of evidence seizure.

Consider the investigation and prosecution of the common email fraud scheme popularly known as the Nigerian or 419 scam, coined because it originated in the West African nation some years ago. A detailed, technical investigation aimed at securing a conviction of a 419 scam would be beyond the operational resources of nearly every police force in the world. In reality, the costs of these investigations are so high that virtually none are within the means of ordinary American law enforcement. Only where losses are extraordinary is enforcement generally viewed as justifiable – and then, only by very large agencies or federal agencies with budgets that can support such action.

Competence

When a detective responds to a homicide scene, one of the first things he does is to make sure that the area is protected from anyone who would change or remove the evidence. Without crime-scene integrity, a jury cannot properly draw conclusions about the crime because neither the investigators nor the evidence will have credibility.

Cybercrime evidence requires the same care and control – but because it exists in such a different form the precautions connected with its discovery, storage, and retrieval are much different. The investigator will be required to establish procedures or protocols which guarantee that evidence from data storage media is unchanged from the time of its seizure or discovery. The cyber forensic investigator will need to put up the electronic equivalent of yellow crime scene tape to make sure that the data is not compromised.

3 http://www.leg.state.or.us/ors/164.html.

4 Council of Europe, Convention on Cybercrime (2001), http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

5 Mueller, Robert S., Statement to Senate Judiciary Committee, December 6, 2006, retrieved March 3, 2007 from http://www.fbi.gov/congress/congress06/mueller120606.htm.

6 Martinez, S. M., (September 22, 2004), "Testimony Before House Government Reform Committee's Subcommittee on Technology, Information Policy," Intergovernmental Relations and the Census, retrieved March 3, 2007 from www.fbi.gov/congress/congress04/martinez092204.htm.

This means that, at a minimum, forensic investigators must have adequate knowledge of computer hardware systems, cyber forensics software, and the typical consumer software that will usually be seized. Additionally, investigators need a solid understanding of the requirements of the relevant constitutional law and evidentiary law. The legal knowledge enables them to conduct their investigations in a way that does not run afoul of suspects' rights – ensuring admissibility of evidence – and in a way that allows them to understand the procedural requirements of evidence seizure (e.g., how to legally obtain subscriber information from an Internet Service Provider).

This expertise must be supplemented by adequate hardware and software resources to enable them to recover electronic data in a way that will allow its admissibility as evidence in the prosecution of criminals (cyber or otherwise). In reality, the competent investigator will become a regional resource for other investigators and prosecutors in cyber forensics investigations.

Requirements for prosecutors, while not as technical, are never-the-less substantial. Prosecutors, at both the state and federal level, are the gate keepers for all criminal cases in the United States. Prosecutors traditionally know little about cyber forensics. While most are computer literate, their training has typically not included much of the technical information they need to successfully supervise cyber prosecutions.

Planning for and prosecuting cybercrime

Because cybercrime will occur in the future, regardless of efforts to deter it, both private and public sector entities must plan to deal with on several levels.

Internally, both public and private entities must plan for the fact that at some time, their employees may use computers and the Internet to commit unlawful acts or acts that warrant discipline. This eventuality calls for internal policies governing the use of company or agency equipment for personal email and Internet use. These policies should clearly and regularly be communicated to employees and should take into account relevant business practices of the entity.

Depending upon the nature of the business, the entity may be required to have its own internal cyber investigation team in place. This may be necessary for business reasons and it also would allow the entity to substantiate any claims it needs to make about internal controls and adherence to good corporate governance.

Shortcomings of old-style thinking

Proliferation of both Internet connectivity and of criminals who exploit the new technology will drive significant changes in law enforcement efforts. Old-style criminal investigations and, more significantly, old-style thinking about crime will fail to effectively address Internet crime. This is true for several practical reasons.

Cost – Only the largest and best-funded investigative agencies have the financial resources to investigate most cybercrimes. While cyber forensics permits some aspects of investigations to occur without travel, the technology does not eliminate the need to put detectives in the place where the crime originated.

Jurisdiction – Particularly in the United States, jurisdictional issues in old-style crime are rare. Liberal extradition between states and interstate cooperation, both formal and informal, expedite investigations in the uncommon cases where criminal activity crosses state borders. All of these advantages evaporate in many cybercrimes, however, because cases with victims in the United States – as an example – may well involve suspects in Eastern Europe or Asia. Even if cost issues are overcome, investigators will have no jurisdiction outside of the U.S. to seize evidence, make arrests, and compel attendance in court proceedings. Returning suspects to face trial, and even determining the appropriate venue for such trial, becomes difficult or impossible.

Education and training – Investigators, prosecutors, criminal defense attorneys and judges typically have adequate training in the law. They typically have little or no training in the technology related to cybercrime. Sometimes this training can be expensive and hard to obtain. And because technology continues to evolve, today's education may become irrelevant tomorrow.

Recommendations

Prevention – While controversial, policy makers will quickly understand that their agencies cannot address every instance of cybercrime. This makes a consideration of prevention important. Selective investigation and prosecution of cybercriminals who perpetrate particular forms of cybercrime may have a prophylactic effect, discouraging would-be cyber criminals.

Cooperative efforts – The very nature of cybercrime and cyber forensics investigations dictates the strong need for cooperative efforts. Cooperation in the area of cyber forensics fits into two general categories: inter-agency cooperation and cooperation between law enforcement and non-law enforcement entities.

Local police departments with trained cyber investigators often make their facilities and experts available for departments without the resources, and on a case-by-case basis departments frequently work together to investigate and prosecute cyber criminals. The U.S. Department of Justice's centralized reporting of cybercrime using the Internet represents a newer technology-based example of inter-agency cooperation that simplifies the processes for victims and may serve as a model for the future.[7]

7 United States Department of Justice, Computer Crime & Intellectual Property Section. "Reporting Computer, Internet-Related, or Intellectual Property Crime" from www.usdoj.gov/criminal/cybercrime/reporting.htm.

Cooperation with non-police entities is somewhat different and can take several different forms. Some investigations cannot occur without cooperation with corporate systems administrators. This is true mainly because detectives can never have adequate training to understand proprietary software and network systems. Without the technical expertise provided by the company's experts, the investigation will fail.

Finally, international legal cooperation is required. Specific treaties and conventions recognizing the benefits of cooperative investigations and prosecutions can facilitate international cybercrime enforcement.

Training – Education relating to cybercrime and cyber forensics must occur at all levels of the judicial system.

At the investigatory level, solving cybercrime cases requires dedicated and trained experts with adequate forensic tools to examine the relevant evidence and protect the rights of suspects. No law enforcement training program can succeed, however, without attention to the training of supervisors in at least the basic levels of cyber forensics. Sergeants, captains and chiefs must have this knowledge to appropriately staff, train, fund, and lead their departments' cyber investigations.

At the legal level, an attorney cannot adequately represent a cybercrime suspect without at least a basic level of computer understanding. While it is true that the attorney can hire experts to aid and assist with criminal defense, the attorney remains in charge of any such process and cannot function successfully without knowledge of the relevant technology. This rationale applies equally to prosecutors who will direct cyber investigations, make charging decisions, and lead the cases through the courts.

Any discussion of the training of legal professionals that does not include mention of judicial training falls short. Judges must possess a strong basic knowledge of computers, the Internet, and cyber forensics. They must make decisions regarding probable cause in the issuance of search warrants and in preliminary hearings, the admissibility of cyber evidence, the appropriateness of expert testimony, and many other significant legal issues. The analysis of old-style evidence does not intuitively carry forward to cyber evidence without an understanding of the nature of such evidence.

Conclusion

The role which cyber forensics has and will continue to play in the successful prosecution of 21st century criminals is at an embryonic stage. The union of computer technology, cyber forensics, and law enforcement is poised for rapid and exciting growth as both technology and the exploitation of technology provide continued opportunities for illegal activities to be perpetrated in a matter of milliseconds from remote geographical distances.

Professionals (law enforcement, attorneys, judges) tasked with prosecuting those who elect to utilize technology to undermine the social rules of acceptable use can no longer accept the status quo and must strive to elevate their level of technical expertise in hopes of remaining at least at par with those whom they pursue and prosecute.

Technology will continue to change, making cybercrime an ever present, evolving, and changing reality, one not destined to go away. By being pro-active, remaining abreast of technological changes, obtaining on-going training in the theories and techniques that define the field of cyber forensics, today's professionals will be better prepared for the challenges of prosecuting tomorrow's cyber criminals.

About the Authors

Kent Mortimore is an attorney and consultant providing training and technical legal advice to prosecutors, judges and professors, Kent currently lives and works in the Middle East. Prior to his overseas assignment, he served for 20 years as a prosecutor in Oregon.

Dr. Al Marcella, Jr., is president of Business Automation Consultants LLC. He may be reached at amarcella@mindspring.com.

Doug Menendez, CISA, CIA, is the IT audit manager for Enterprise Rent-A-Car and an adjunct professor at Maryville University. He may be reached at douglas.menendez@erac.com.

This material originally appeared in and has been condensed for publication here from Chapter 12 "Cyber-Forensics and the Changing Face of Investigating Criminal Behavior," which was developed by Kent Mortimore for inclusion in *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes* - Second Edition, written by Al Marcella and Doug Menendez, published by CRC Press, www.crcpress.com.