Local Law Enforcement and its Digital Forensics Future

by

Ron Coopman

Westminster Police Department

May, 2008

Command College Class 42
The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).
Local Law Enforcement and its Digital Forensics Future

Digital forensics is the collection, examination, preservation and recording of information found on computers and information networks. It is an increasingly evolving and complex area of criminal and civil investigation that has been on the rise for more than two decades, and whose importance to law enforcement will continue to grow exponentially over the next ten years. Public safety and local policing agencies in particular must take aggressive steps to prepare for changes in how crimes are investigated and solved. Without understanding the complexity of digital forensics and how it influences all crime, law enforcement leaders will be behind the curve to solve crimes swiftly and precisely in the future.

The world around us is changing, and so are the tools used by present-day suspects. With the dynamics of digital forensics in place, it begs the question; do smaller agencies with limited resources close shop and farm out their digital investigations? Do they maintain investigations in-house? Or might there be a hybrid of the two? Although each individual agency must make the decision that is right for them, in varying degrees a hybrid model will likely develop in most law enforcement agencies of the future.

Technology Explosion

Since the 1970’s the evolution of computer technology has changed how the world conducts its business. Most commerce and commercial transactions are now done through electronic transfers. Personal computers are in virtually every home and business, and corporations
frequently have networks consisting of thousands of integrated computers. Email and text messaging have practically replaced how we communicate with each other and personal communication devices with email, video and camera capabilities are commonly used by elementary school-aged children. All of these electronic storage devices have a potential to leave a permanent trace of stored information and thoroughly document the activities of the user.

To put the sheer number of digital devices into perspective, one need only look at the wireless communications industry. According to CTIA-The Wireless Association (CTIA, January 23, 2008) there are more than 243 million wireless customers in the United States. Wireless communications customers grew by 24 million subscribers in just one year, and the wireless penetration stands at 80 percent of the U.S. population. This number has grown from 2005, when there were a mere 194.5 million wireless users. The average user is now upgrading or changing their wireless phones every 12 months. When one considers adding personal computers, flash drive, MP3 players and cameras into the mix, the sheer amount of digital gadgetry which could be used by criminals is quite overwhelming.

Every transfer of data through these electronic devices leaves a trail of information that can potentially be retrieved through forensic examination. Each time a computer is accessed, traces of the users activities are almost always left behind. Nearly every key stroke, deleted file and entry into the internet is recorded and stored, leaving a wealth of evidence for the trained investigator to find. When used for illicit purposes, the computer, network or data system essentially becomes a crime scene; one that is very unlike crime scenes of the past. Computers
and data systems have made criminal activity exceedingly lucrative for criminals whose only limitations are their computer aptitude, creativity and the degree to which law enforcement is prepared to deal with it.

Until now, most law enforcement agencies have tailored their computer forensic responses to meet their individual departmental needs; many have experienced moderate success conducting digital forensic examinations. For instance, the Westminster Police Department (CA) started by creating a Computer Forensics Lab in 2001 using available workspace and personnel. The investigators assigned to the lab were primarily assigned to other major crime details. The initial demand for digital forensics was low compared to today’s standards. The assigned detectives honed their skills and gained experience as digital forensics examiners on high profile cases such as homicides and child pornography cases. Since the assignment itself was collateral, there was little time available for active high-tech crime investigation or probation/parole violations. In 2007, department staff recognized the emerging trend and responded by assigning full-time investigators into the unit, multiplying the agency’s digital forensics capacity and effectiveness.

Conversely, some agencies have elected not to do anything at all and rely on other local agencies, a regional task force or county services for their digital forensics services. But the reality is that the total amount of seized digital evidence is rapidly increasing each year. Clearly, some cases will not rise to the minimum threshold requirement for outsourcing to an outside agency, and the evidence that is outsourced will likely take an extended period of time for
processing. This is prompting law enforcement agencies of all sizes to look for new ways to increase computer forensic capacity in the face of limited or shrinking resources.

**Historical Background**

Structured programs designed to study computer data for use in criminal prosecutions have been in existence for many years. In 1992, the FBI established the Computer Analysis and Response Team (CART) and charged it with the responsibility for computer analysis (Whitcomb, 2008). The CART assumed primary FBI responsibilities for search and seizure of computer evidence as well as forensic examinations and technical support for FBI investigations. The CART program was developed primarily for federal prosecutions and did not diminish the burden of processing digital evidence on state and local agencies.

Few agencies were fortunate enough to employ computer-savvy law enforcement officers who had the technical knowledge and foresight to collect, preserve and examine electronic data for criminal prosecutions (Spruill, 2008). Formal government-sponsored training programs did not exist, so the investigators relied heavily upon private-sector training programs. According to Spruill, when local investigators became proficient in computer forensics, they were relentlessly pursued and recruited by federal policing agencies and the private companies who specialize in civil computer forensic investigations. The combination of computer skills and investigative experience was highly preferred by private companies and readily found in state and local law enforcement agencies. Efforts to organize the computer forensic discipline on a wide scale basis were largely unsuccessful until the late 1990’s.
In 1998, the Scientific Working Group on Digital Evidence (SWGDE) was formed by The Federal Crime Laboratory Directors group (Pollitt, 2003) and tasked with bringing together federal agencies who were involved with the analysis of digital evidence (Whitcomb 2008). Representatives from various state law enforcement organizations were invited to the meetings. Soon thereafter, the group partnered with the American Society of Crime Laboratory Directors/Laboratory Accrediting Board (ASCLD/LAB) with the goal of accrediting a new forensic discipline to join other established forensic sciences. The partnership provided the energy needed to thrust digital forensics in the direction of full scientific recognition and accreditation.

Lab Accreditation

ASCLD/LAB began accrediting forensic labs beginning in 1982. Since then ASCLD/LAB has accredited labs in the forensic disciplines of Biology (DNA) Controlled Substances, Crime Scenes, Firearms and Toolmarks, Latent Prints, Questioned Documents, Toxicology and Trace Evidence. The Digital Evidence Discipline was accredited by ASCLD/LAB in 2003 and divided into 4 subdivisions: Computer forensics, Audio Analysis, Video Analysis and Imaging Analysis (Barbara 2004). All of the listed forensic disciplines have enjoyed widespread acceptance in the scientific community.

The 1993 court case Daubert Fry vs. Merrell Dow Pharmaceuticals, Inc. 509 U.S. 579 (1993) set the standards upon which forensic labs are certified. The Daubert court ruled that judges were to
be the “gatekeepers” of scientific testimony (Whitcomb 2008). The basic Daubert rule is the reasoning or methodology underlying the court testimony must be scientifically valid. Scientific conclusions of traditional forensics analyses and the information of computer forensic science are distinctive forensic examinations. Both must produce valid and reliable results from state-of-the-art proceedings that are detailed, documented, peer-reviewed and from protocols acceptable to the relevant scientific community (ASCLD/LAB 1994).

ASCLD/LAB offers two accreditation programs in their laboratory accreditation program. The Legacy Program is the original ASCLD/LAB laboratory accreditation program, and the more difficult International Program was recently approved by the ASCLD/LAB organization in April 2004. As of February 2008, ASCLD/LAB has accredited 337 public and private crime labs worldwide. The list of accredited laboratories includes 178 state laboratories, 103 local agency laboratories, 22 federal laboratories, 10 international laboratories and 24 private laboratories. Of the 337 accredited labs, 55 are accredited under the International Program and 282 are accredited under the Legacy Program (ASCLD/LAB 2008).

To be accredited through the ASCLD/LAB process, the labs must undergo a rigorous review of their internal quality control systems to insure they produce technically valid results. There are 145 basic requirements in the Legacy Program, and 380 basic requirements for certification through the International Program (Barbara, 2004). Accreditation is voluntary and open to any forensic crime laboratory which believes its management, operations, personnel, procedures, equipment, physical plant, security and health and safety procedures can meet the established
standards and criteria from the program selected (Barbara 2008). International standard labs must meet all applicable benchmarks to receive certification.

As of February 2008, there were twenty-two (22) laboratories accredited by ASCLD/LAB in Digital and Multimedia Evidence (Whitcomb 2008). There are eighteen (18) local, state and federal labs accredited in the Legacy Program, and four accredited in the International Program. The four International accredited labs include the DEA Digital Evidence Laboratory; the FBI Digital Evidence Laboratory; the Charleston (South Carolina) Police Department’s Forensic Laboratory and the Utah State Crime Laboratory (Whitcomb 2008). In January 2008, Texas-based Hill Schwartz Spilker Keller (HSSK) became the first U.S. digital forensic lab to obtain Legacy Program certification for ASCLD/LAB (ProSecurityZone, 2008). Very few of the private labs are certified International, and those who have been certified are genetic/DNA labs (Spruill, 2008).

The International Program is a much more arduous process for certification, since it uses the ISO/IEC 17025:1999 (E) standard as the basis for accreditation. The ISO/IEC 17025:1999(E) is an internationally recognized standard which contains the requirements testing and calibration labs must meet to show their labs have quality control, are technically proficient and produce valid results (Barbara, 2004). When one considers the complexity of accrediting a digital forensic lab, opening and operating one can be a very daunting task for any single agency to attempt. Since very few agencies could afford the resource commitment, many looked for external opportunities to increase their digital forensics capabilities.
The limited supply of trained investigators and the costs associated with forensic equipment and software prompted policing agencies to begin coordinated efforts to share assets and resources through task force agreements. In 1999, the first-of-its-kind San Diego Regional Forensics Laboratory (RCFL) was established providing an investigative resource for San Diego, Imperial and Riverside Counties. The RCFL personnel included investigators and agents from local, state and federal law enforcement agencies. The RCFL model worked, prompting the sudden expansion of more RCFL programs. There are now 14 RCFL task forces operating throughout the United States (Hendron, 2005). The FBI expects to open a 15th RCFL in 2008 and is currently undergoing review of potential RCFL site proposals. Many of the FBI RCFL’s are accredited through the ASCLD/LAB Legacy Program.

Cost Considerations

Operating a digital forensic lab can be an extremely costly undertaking. In FY 2004-2005 the San Diego County Computer and Technology High Tech Crimes Task Force (CATCH) spent more than $300,000 on costs directly related to computer forensics activities, training, overtime and equipment; all for only six investigators (Hendron 2005). But these costs are minimal when compared to the start-up costs of a fully-equipped FBI RCFL. Each RCFL lab costs about $3 million to open, not including the certified staff members and their salaries. Secret Service Deputy Director Brian Nagel stated “law enforcement has been propelled into technologically non-traditional terrain requiring highly specialized skills and innovative applications of traditional investigative strategies. It is imperative to address the changes in technology by
providing training on cyber-investigative techniques and by sharing current expertise among Federal, State and local officers.” (Homeland Security Press Release, March 9, 2007)

Resources of the RCFL can be utilized by local agencies for state cases; however, the regional lab model does not work for local police agencies in every case. Westminster Police Department Digital Forensic Examiners Andy Spruill, Tommy Rackleff and Glenn Finley all agree a contingent digital investigative force must remain in place at the local level to handle active investigations in areas such as probation violations and cases where time is critical in the retrieval of digital evidence (i.e. the first 48 hours after a homicide). RCFL’s and regional labs frequently handle state cases for local policing agencies, but the examinations are prioritized based on an established set of criteria.

Local Labs

Currently, state and local policing agencies have the ability to conduct digital forensic examinations, but lack training, equipment and resource commitment to fully implement computer forensics on a widespread basis. Costs remain prohibitive for most agencies who desire their own computer forensics capability. According to Jimmy Doyle, former executive officer of the NYPD computer investigations and technology unit and current director of Northeast operations for Guidance Software, the decision to train internal staff is about cost-benefit and risk-management analysis. Doyle says agencies can expect to spend about $30,000 for one machine and the software to conduct simple exams, and an additional $5,000 to $10,000
per year per person on training and travel (Duffy, May 2004). The price does not include ongoing costs such as salaries and supplies.

Private Industry

With the criminal computer forensics industry workload demand high, and the supply of trained investigators low, private companies have sought to take advantage of the shortage by contracting services to various agencies. Some of these private companies have been in the computer forensics business for many years and provide a substantial amount of training, equipment and software to law enforcement. The dominant player in the forensics software business is Pasadena-based Guidance Software (Reagan 2006). Guidance Software trains about 3,500 law enforcement officers every year.

Andy Spruill, who oversees the Guidance Software consulting division, said that computer forensics is still a specialty, with few people having the skills and resources to do it. Finding good criminal investigators with the technical skills to master computer forensics is a challenge (Spruill 2008). Although there certainly are more technologically savvy police officers than there were 10 years ago, certain skill sets, formal education and certifications in specialized software are required of today’s digital forensic examiner. Finding the officer with the aptitude is only the first step in the search. A civilian alternative, someone who is already a certified digital forensic technician but not a sworn police officer, may lack the criminal investigative background to recognize evidence when they see it. This required combination of skill sets is really where the pool of available qualified examiners gets shallow (Finley, 2008).
Mark Graff, Chief Cyber Security Officer at the Lawrence Livermore National Laboratory identified three necessary skill sets in his forensic officers. The first is technical skill, an understanding of how data is stored and retrieved, and knowledge of the tools that are used. Second, is sound training in the legal requirements of evidence gathering and presentation; the procedures that investigators need to observe and preserve the chain of evidence and remain within the parameters of the law. Finally, investigators must have a good understanding of how people use and misuse computers (Duffy, May 2004).

Mid-sized policing agencies like the Westminster (CA) Police Department have been in the computer forensics business for several years. The Westminster forensic lab can conduct most types of examination on digital evidence with some limitations. Staffed with one full-time investigator and two part-time investigators in a small 300 square foot room, the lab team examines an average of 30 pieces of evidence each month. Evidence can range from digital phones and PDA’s to large capacity computers holding terabytes of information. Evidence processed through the lab can vary. The lab has handled critical evidence seized in homicide investigations to probation violation cases and everything else between. Additionally, investigators are responsible for wiping critical data such as stolen personal information or illegal pornography from any evidence or property item before it is released to citizens.

The enormous amount of information contained within computer hard drives requires the Westminster lab to prioritize its workload. It is impossible for investigators to examine every
piece of data contained within seized evidence. Twelve gigabytes of printed text data would create a stack of paper 24 stories high. For practical reasons, computer forensic science is most effective when only the most probative information and details of the investigations are provided to the examiner (Noblett, Pollitt and Presley, 2000). With one full-time police investigator and two part-time digital forensic experts on staff, the Westminster Lab combines an optimal mix of investigative experience and forensic science knowledge. This combination enables Westminster PD to make best use of its resource and space constraints. Under the current state of affairs in the criminal justice system, forensic labs similar to Westminster’s are effective and will continue to meet most investigative demands of their agency.

**RCFL versus Local Labs**

As RCFL’s continue to open throughout the country and increase capacity to process digital evidence in most federal court jurisdictions, the FBI has communicated its desire to impose new evidence guidelines for federally prosecuted cases. By 2010, the FBI will require that all digital evidence in federal cases be examined in ASCLD/LAB certified laboratories (Spruill 2008). Since RCFL’s are ASCLD/LAB Legacy Program certified, evidence handled through FBI RCFL’s will not be impacted. Local policing agencies operating forensic labs and participating in criminal investigations where federal prosecution is possible would be affected. The number of locally investigated cases requiring federal prosecution can vary from agency to agency, so the degree of impact on all agencies as a whole is difficult to determine. Detective Finley (2008) estimated the Westminster Police Department would experience moderate impact, since roughly 60 percent of the digital forensic cases handled by him are fraud, forgery or narcotic related
cases having the potential of involving federal law enforcement authorities. RCFL’s will also see their workloads increase substantially. In 2005, the 200-plus examiners at the FBI RCFL labs analyzed more than 1,400 terabytes of data, equal to a stack of paper 47,000 miles high (Reagan, 2006).

The proliferation of regional labs is an essential piece of law enforcement’s digital forensic future, but it is not the panacea that many believe. Regional labs and RCFL’s provide a critical service to federal, state and local agencies that investigate crimes with federal implications. Policing agencies with non-accredited digital forensic labs must not abandon their ability to process digital evidence at the local level. Those who have yet to establish an internal digital forensics capability must critically consider the costs and benefits of having one. The advantages of having an in-house capability include immediate processing of time-critical evidence, lowering the risk of mishandling evidence, and providing a mechanism for investigators to scan potential evidence to determine evidentiary value without bogging down a regional lab.

Locally operated digital forensic labs must have trained and certified personnel conducting forensic examinations, even though the labs have not been certified. The investigator/examiner frequently gives expert testimony in federal court. This occurs because the types of criminal acts involving digital evidence are commonly accomplished with the transfer of electronic digital data through the internet. Since the internet knows of no boundaries, it is common for investigations to begin locally and suddenly cross a national or international jurisdiction triggering involvement
of federal law enforcement. Under the current FBI policy, evidence examined by local examiners/investigators can be admitted into federal court without examination in an accredited lab. The established requirement is that local examiners/investigators must provide their qualifications in court and must present their expert testimony each time they appear on a case. It is quite a burdensome process, but effective nonetheless. It is the only means for forensic investigators from non-accredited labs to provide expert testimony in court.

With the new requirements imposed by the FBI, local law enforcement will no longer be allowed to present evidence examined at a non-certified lab into any criminal federal proceeding. Since only evidence obtained through ASCLD/LAB certified laboratories will be allowed into evidence, local investigators/examiners must conduct a litmus test on each case and make a determination if the case has potential to escalate to the federal level before any forensic examination takes place. If the potential is there, the investigator must package the evidence and send it to the FBI RCFL for analysis. This will create a huge change from current practice, and will force the local agencies to change their practices.

Conclusion

With the new federal evidence requirements, RCFL workload will increase immensely. Any criminal case that has the potential to go federal will not be investigated by local forensic examiners. Instead, they will evaluate the case potential, and if a federal crime is involved, the evidence will be packaged and sent to a regional certified lab. This equates to twenty-two ASCLD/LAB certified labs examining all federal crimes evidence, a marked change from
current policy. Local non-certified labs such as Westminster’s lab will still be allowed to conduct examinations on evidence seized for state crimes. Local agencies can still rely on their own labs until they are forced into certification to make the evidence more scientific and believable. Changes in state courts are not expected in the near future, but it will eventually be more difficult for local examiners to admit evidence into court as the criminal justice system becomes more educated in digital forensics. Criminal attorneys and judges will become more knowledgeable and will ultimately demand more structure in local computer forensic labs. When this occurs- and it will, local agencies will be forced to develop minimally accepted standards similar to ASCLD/LAB requirements.

All forensic disciplines have undergone similar evolutionary changes on their way to widespread acceptance. If we consider where DNA/genetics were ten years ago, it is not difficult to understand how quickly a forensic science discipline can evolve. Law enforcement must focus on the near future and understand the enormity of forensic resources required to investigate future crimes and the importance digital forensics training will have on the profession.

References

American Society of Crime Laboratory Directors/Laboratory Accreditation Board


http://www.dhs.gov/xnews/releases/pr_1173477460607.shtm


Spruill, Andy. Manager of Consulting Division, Guidance Software. Personal communication dated Thursday, March 6, 2008.

Whitcomb, C.M., The Police Chief. (February 2008) *The Evolution of Digital Evidence in Forensic Science Laboratories*. Available at:

[http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1321](http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1321)