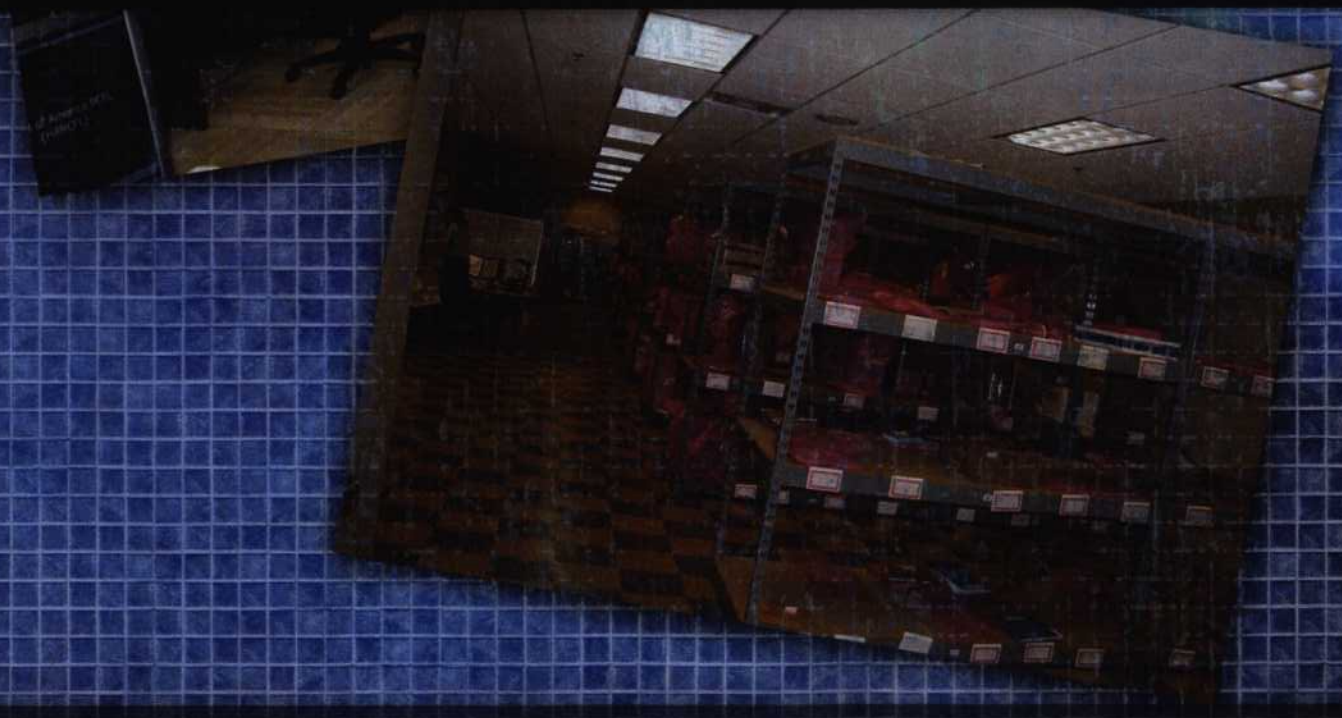
Kansas
GOVERNMENT JOURNAL

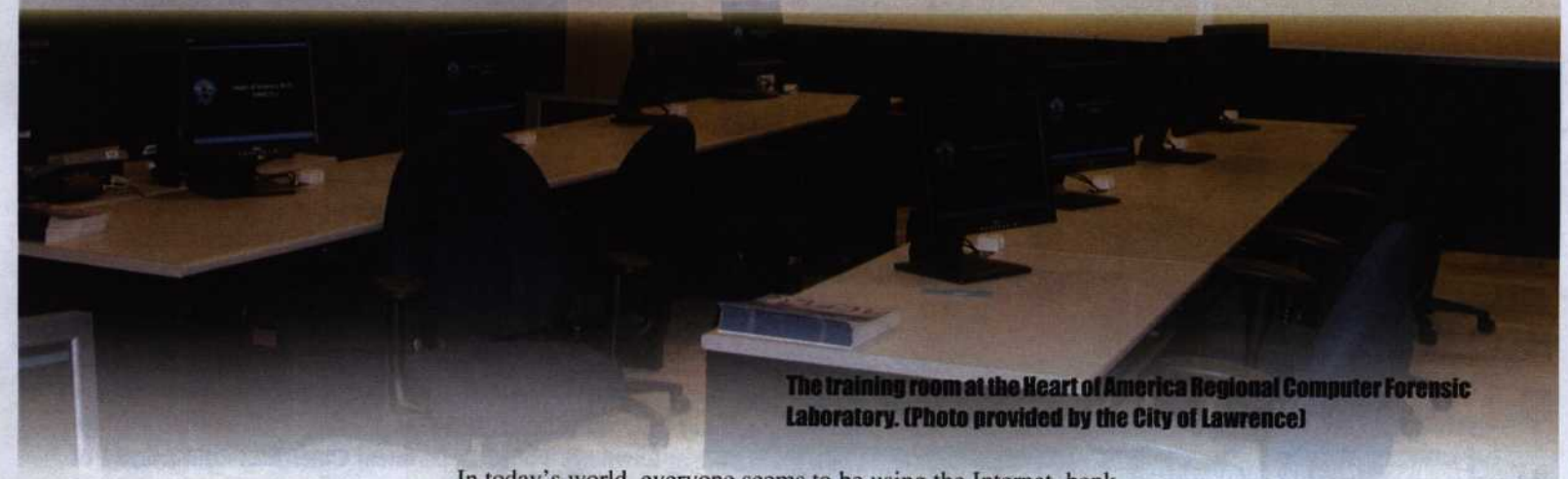
VOLUME 92 - NUMBER 12 DECEMBER 2006

HIGH TECH CRIMINAL INVESTIGATION



Heart of America Regional Computer Forensics Laboratory: Cooperation Furthers Law Enforcement

by Lisa K. Patterson



The training room at the Heart of America Regional Computer Forensic Laboratory. (Photo provided by the City of Lawrence)

In today's world, everyone seems to be using the Internet, bank card, cell phone, PDA or a pager, each leaving a digital trail. These digital devices have created a whole new realm of police work including criminal investigations involving digital evidence. Forensic investigations or police work to establish facts or evidence that can be used in a court of law have a long history with chemists and blood spatter experts and today forensic media examiners are playing a vital role in many investigations.

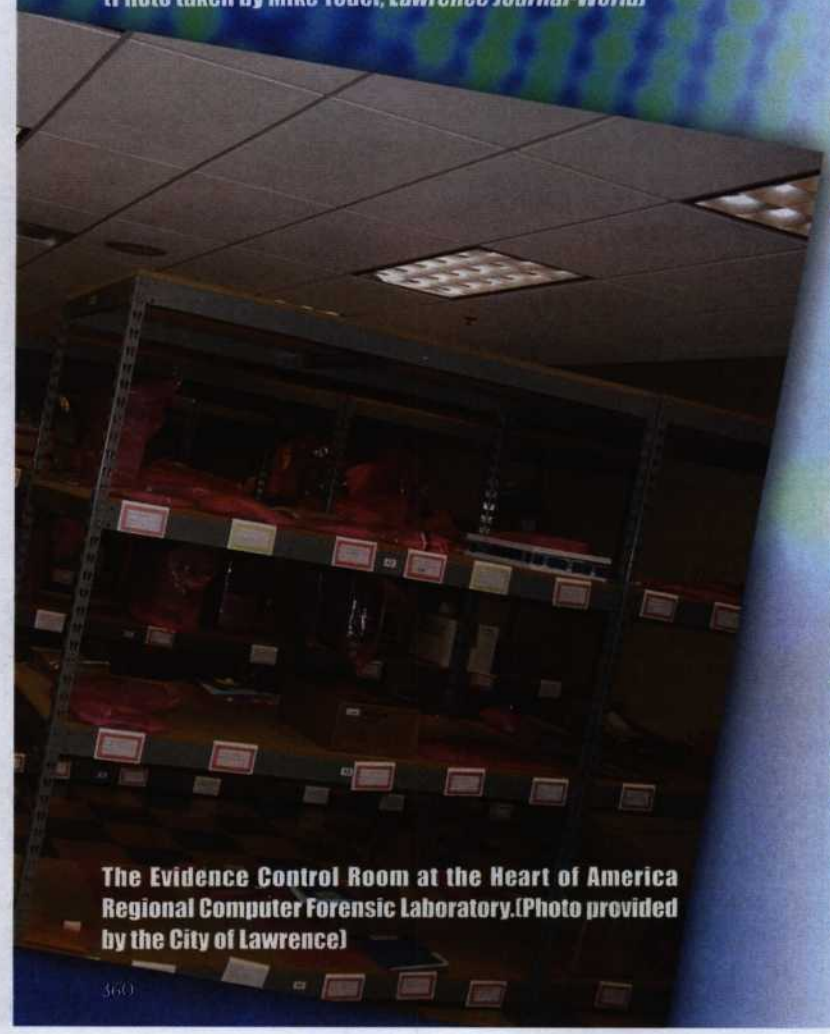
The need for police departments and the law enforcement community to develop resources to support forensic investigations on digital evidence has grown. Today, many individuals use a computer similar to the use of a diary or journals in the 19th Century. Computers have a tremendous ability to store information and often the police have a need to retrieve that information during an investigation. Many crimes investigated today are related to pornography, an area of criminal activity that is being supported by the Internet.

Digital evidence can be present in many types of criminal investigations. There is documented use of computers by terrorists. The ability for individuals to plot attacks and share the information is greatly aided in the computer age. In World War II, the Federal Bureau of Investigation (FBI) opened letters, the means of transferring information. Today, those letters are now electronic and the transferring of information is done with the stroke of a key or the click of a mouse. Criminal investigations of theft or destruction of intellectual property, fraud, Internet crimes, and murder are entering into the digital forensic laboratory environment on a routine basis.

Regional Computer Forensic Lab

There are 867 local, state and federal agencies in Kansas and the western two-thirds of Missouri that can look to the Heart of America Regional Computer Forensic Laboratory (HARCFL) for assistance with digital evidence. There are 20 full-time examiners

Lawrence Police Detective Dean Brown presents evidence in Thomas E. Murray's murder trial in Douglas County District Court. The prosecution touted recovered searches from Murray's computer as proof Murray killed his former wife, Carmin D. Ross, in November 2003 at her home in Lawrence. (Photo taken by Mike Yoder, *Lawrence Journal-World*)



The Evidence Control Room at the Heart of America Regional Computer Forensic Laboratory.(Photo provided by the City of Lawrence)

assigned to the HARCFL, who provide complete forensic exams of digital evidence and assist in executing search warrants and training law enforcement officers—all at no cost to the requesting agencies.

The growth in the number of investigations involving digital evidence is seen in the lab's demand for services. Currently, the lab has a 6-month backlog and is expected to work on 425 to 450 cases this year, up from 325 cases in 2005. The analogy of "searching for a needle in a haystack" fits much of the lab's work. In a single case, there were over 1,200 pieces of media to be examined.

The HARCFL is a place where the FBI is sharing years of work, technology and experience with state and local agencies. The FBI's Engineering Research Facility and the Operational Technology Division provides cutting edge technology to the labs. The regional lab places resources and training in the field at a level that could not be matched using the traditional FBI structure. Established in 2003, the Heart of America Regional Computer Forensic Laboratory is 1 of 14 labs in the nation with 16 participating agencies. It is operated with funding from the FBI and available grants.

City of Lawrence Involvement

When Lawrence Police Department Chief Ron Olin learned of the opportunity for the department to participate in the regional computer forensic lab, he was interested in the unique structure. Unlike a taskforce, the regional lab had the potential to demonstrate an unmatched level of cooperation between federal, state, and local agencies. He also recognized that the Department's own forensic unit would benefit from the training and research conducted by the lab. Once the City signed the memorandum of understanding with the HARCFL, the Chief assigned one detective full time to the lab, Dean Brown. Brown learns from the work that is underway in the regional lab and can identify the most efficient equipment, policies, and procedures to benefit the Lawrence Police Department.

While Detective Brown has been the single participant from Lawrence assigned to the lab, the agency has the opportunity to rotate the participating detective. While there is a need to maintain consistency with examiners assigned to the lab, the HARCFL requires a minimum commitment from each examiner to realize a return on training and education provided. Detective Brown has been working at the lab for just more than three years and is likely to be replaced by another Lawrence Police Department representative in the coming year.

Lawrence has had the opportunity to use the resources provided by the lab. In one instance, the Department was investigating computer programmers suspected of wrong doing at a Lawrence company. With the assistance of the lab, the operations of the company continued uninterrupted while the criminal investigation was underway. When the investigation was completed, felony charges were sought rather than nuisance charges. The sophisticated response to this complex criminal activity was made possible, in part, by the personnel and training resources of the regional computer lab.

The Role of a Digital Evidence Forensic Examiner

The duties of the examiner include completing examinations of digital evidence, presenting evidence in court, providing immediate

responses to investigations across the region, and providing technical support such as suggestions for search warrant language and instructions to preserve digital evidence.

It takes approximately one year for preliminary education to be completed by a participating agency's staff and to become a certified digital forensic examiner. During that training, he or she becomes as proficient as a network technician who has been in the field for six months. He must also complete examinations under the supervision of a certified examiner and pass a competency test. In addition, examiners are required to complete annual training and are often involved in specialized training all requiring competency testing at the end of the course.

Governing the Regional Forensic Laboratory

Governed by a local executive board similar to a board of directors, the lab is currently guided by Chief John Douglass of the Overland Park Police Department who serves as Board President and Lawrence Police Chief Ron Olin who serves as Treasurer. The Board sets the pre-screening process for each examiner and assists with the interviews of examiner candidates. The Board is responsible for the management and daily operations of the lab, as well as overseeing the lab's director and approving expenditures.

The Board has also been involved with the accreditation through the American Society of Crime Laboratory Directors. An internal audit was recently conducted by the FBI. The executive board weighed in on the local and regional needs of the agencies. Sister labs in New Jersey and California, where there is high density of digital evidence, may serve a geographic area of a single city or county. In the Midwest, the Board advocated for the flexibility to support local and state agencies that may be several hundred miles away.

Participating agencies are making a substantial investment with staff wages and benefits; however, the benefits can also be substantial. The regional lab has the infrastructure in place to address all of law enforcement's digital forensic needs and provides access to millions of dollars of equipment. The lab has also developed and continues to update standard operating procedures for conducting examinations in a scientifically sound manner. A second agency benefit is the exchange of information about technology options. Digital evidence is new and constantly evolving. It is extremely expensive to stay abreast of trends and advancements. Having access to the research and recommendation of federal agencies and the HARCFL is a valuable asset when local agencies are making purchasing decisions for their forensic units, assigning investigators, and planning department futures.

Additional information regarding the Heart of America Regional Computer Forensic Laboratory and cases worked by the laboratory is online at www.harcfl.org.

Lisa K. Patterson is the Communications Manager for the City of Lawrence and can be reached at lpatterson@ci.lawrence.ks.us or (785) 832-3406.

Murray Homicide Investigation

In March 2006, a Douglas County jury found Thomas Murray, a Kansas State University English professor, guilty of stabbing and beating his ex-wife, Carmin D. Ross, to death in November 2003. A *Lawrence Journal-World* story on the case reported, "Two jurors who spoke after the verdict said there wasn't a single piece of evidence that caused them to convict Murray. Rather, it was the combination of all the circumstantial evidence. Jurors also said Murray's murder-related Internet searches—for terms including 'how to murder someone and not get caught'—were incriminating."

Details of those Internet searches were discovered during the forensic investigation of Murray's computer. Detective Dean Brown, Lawrence Police Department, presented the evidence in court. He described the work completed during the digital evidence investigation as similar to what other forensic disciplines contribute to a criminal investigation. "A chemist and a blood splatter expert as well as digital investigators provide tools for those who are the boots on the ground and who ultimately solve the crimes. The Murray case was solved by the investigators working the case while assistance from the forensic investigators along with physical evidence people helped present the case at trial."

In the Murray investigation, the Lawrence Police Department assisted the Douglas County Sheriff's Office at the crime scene and with the investigation beginning with a victimology, or the profile of all the knowledge about the victim. In today's environment, computers hold a tremendous amount of personal data, data that was traditionally written down or kept in a daily planner. Investigators also contributed language for search warrants to include computers.

Once the suspect's computers were obtained, investigators began to review the Internet history and generate a report with dates and search terms. In trial, Detective Brown conveyed his work and the work of the other digital evidence investigators to the jury. During trials, presenters must be sensitive to the level of computer experience and knowledge of each jury member. One individual may not have any exposure to using a computer while another may be well versed in a computer's operating system. The goal for the detective is to take an abstract idea and create a concrete understanding and of how the investigators drew conclusions so that jurors can draw his or her own conclusion.