

RCU

REGIONAL COMPUTER FORENSICS LABORATORY PROGRAM



Fiscal Year 2004 Annual Report



REGIONAL COMPUTER
FORENSICS LABORATORY
NATIONAL PROGRAM OFFICE



Foreword

This report chronicles the accomplishments and progress of the Regional Computer Forensics Laboratory (RCFL) Program during Fiscal Year (FY) 2004. During the past fiscal year, we prepared for the opening of nine additional facilities across the country, while growing and enhancing the services already offered by our four operational RCFLs in San Diego, California; Dallas, Texas; Chicago, Illinois; and Kansas City, Missouri.

In FY04, we made great strides toward strengthening law enforcement's digital forensics capacity nationwide—a primary goal of the program. We continue to meet this objective by expanding our training offerings, developing new computer forensics tools and technologies, and forming more partnerships with a diverse array of law enforcement agencies. This unique combination—making high technology and state-of-the-art training available through partnerships—absolutely works—as this report describes in further detail.

Finally, it is important to note that the milestones and progress achieved during FY04 are directly attributable to the hard work, dedication, and ingenuity of our RCFL staff members. I am proud of their many contributions—they are the backbone of this program. As always, we remain deeply committed to sharing our resources with all of law enforcement—it is our responsibility as America's premier computer forensics laboratory network.

—Douglas A. Schmidtknecht
Unit Chief
RCFL National Program Office



Table of Contents

PART I: Program Overview

Introduction.....	I
RCFL Services	3
Program Accomplishments for FY04	6
Supporting Law Enforcement—RCFLs in Action.....	8
FY04 Funding.....	9
Training.....	10
Research, Development, Tool Testing, and Validation	13
National Steering Committee	14
On the Horizon for FY05	16

PART II: RCFL Profiles

San Diego RCFL	20
North Texas RCFL	22
Chicago RCFL.....	24
Heart of America RCFL	26
Acknowledgments.....	28



Introduction

As FY04 came to a close, the RCFL Program marked its five-year anniversary—five years of significant accomplishments. During this time, the program's major milestones have included—

- Doubling the number of RCFLs
- Developing and implementing new digital forensics technologies
- Providing much-needed training and equipment to law enforcement personnel (whose only opportunity to receive such resources is through this program)
- Making available full-service digital forensics support to more than 1,000 law enforcement agencies in nearly a half-dozen states.

In 1999, the RCFL Program began as a pilot project—a coalition of law enforcement agencies based in San Diego combined their resources to open a digital forensics laboratory. The San Diego RCFL was created in response to the overwhelmingly high demand for digital forensics expertise and quality services in the region. After the successful launch in San Diego, three additional RCFLs were established in Dallas, Texas; Chicago, Illinois; and Kansas City, Missouri. In FY05, nine more facilities will open in Buffalo, New York; Dayton, Ohio;

Today, nearly every case involves digital evidence of some sort—whether it's from a computer, cellular telephone, video camera, or personal digital assistant.

Denver, Colorado; Hamilton, New Jersey; Houston, Texas; Menlo Park, California, Philadelphia, Pennsylvania; Portland, Oregon, and; Salt Lake City, Utah.

As we reported in last year's inaugural edition of this publication, many law enforcement agencies throughout the country are struggling to keep pace with the demand for digital forensics expertise. This situation remains a formidable and ongoing challenge for all law enforcement because nearly every case involves digital evidence of some form—whether it's from a computer, cellular telephone, video camera, or personal digital assistant (PDA). All of these devices—and more—have the capacity to store valuable digital evidence, yet it takes specialized expertise to extract this data. Often, however, gaining this expertise requires an investment in training and equipment that many law enforcement agencies lack. The RCFL Program is working to fill this void, as this report illustrates.

Highest-Quality Digital Forensics Services

It is often said that RCFLs provide “the highest quality digital forensics services” available to law enforcement. What does that mean exactly? North Texas RCFL Director Michael S. Morris explained it this way, “High-quality services means having trained personnel that follow standard operating procedures. This is in addition to having both quality and peer review measures in-place that ensure our products are as accurate as possible.” Heart of America RCFL Director Thomas J. Maiorana agreed and went on to say, “We follow all of these procedures so that our customers will have confidence in

the products we provide them.” San Diego RCFL Director Randall L. Bolelli described a quality examination as “fully addressing the customer’s request and operating with the highest level of integrity so that the results hold up in court,” and Rick Voss, Director of the Chicago RCFL, emphasized consistency, “RCFLs are setting a standard for how examinations should be accomplished through training, equipment, etc. By doing so, we can explain in court what we did and how we did it. Quality means having repeatable, verifiable, and consistent results.”

“The RCFL Program is deeply committed to providing the highest quality digital forensics services to the law enforcement community. Our record speaks for itself—our findings have stood up in court—resulting in scores of criminal convictions. This is our mission—and it is something of which we can all be proud.”

—Kerry E. Haynes
Assistant Director,
Operational
Technology Division



RCFL Services

An RCFL is a one-stop, full-service forensics laboratory devoted entirely to the examination of digital evidence in support of criminal investigations, such as, but not limited to:

- Terrorism
- Child pornography
- Crimes of violence
- The theft or destruction of intellectual property
- Internet crimes
- Fraud

Types of Assistance

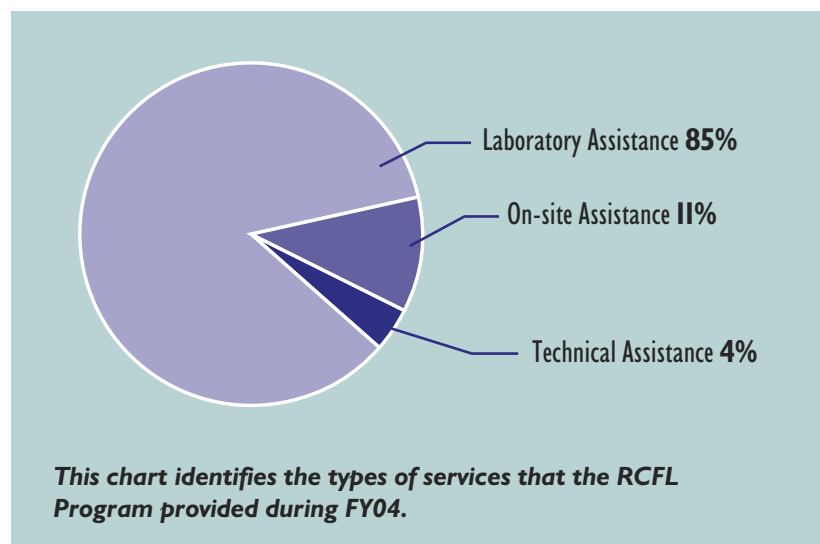
The RCFL Program offers technical assistance in three different areas—

On-Site: This type of assistance requires an Examiner to be physically on-site during a criminal investigation. While on-site, the Examiner can assist with seizing electronic equipment or copying files from an electronic device without having to remove the equipment. During FY04, some RCFLs reported a drop in on-site service requests, specifically for residential searches. This may be because law enforcement is becoming more skilled in identifying

and preserving digital evidence, as well as conducting on-site seizures, thanks to the training provided by the RCFL Program. The program is pleased with this trend because it enables the Examiners to focus their efforts on activities in the laboratory. Conversely, some RCFLs report that their services remain in strong demand for large scale business searches—with some judges requiring Examiners to conduct on-site searches and imaging activities in a limited time or prohibiting their activities all together. The RCFL National Program Office (NPO) is keeping a close watch on this trend because it could impact the law enforcement community as a whole.

Laboratory: A majority of the RCFL's work is conducted in the laboratory and typically involves a thorough examination of the electronic device(s) in a controlled environment. On average, an examination takes 30–90 days to complete; however, complex cases may require more time.

Technical: Any law enforcement agency may consult with RCFL personnel for assistance with preparing a search warrant or affidavit, technical assistance, or advice pertaining to the seizure of electronic equipment, potential searches, or digital evidence.



Best Practices for a Quality Exam—What Every RCFL Customer Should Know

RCFLs are dedicated to offering the most professional, high-quality expertise to their customers. To help the RCFLs provide the level of digital forensics service its law enforcement customers have come to expect, the RCFL Directors cite the following “best practices”—

Meet With the RCFL Staff at the Beginning of an Examination—

Once digital evidence is brought to the RCFL, the investigator should either meet in person or personally speak to the Examiner over the telephone regarding the scope of the examination (e.g., what is the investigator asking the Examiner to search for—e-mails, Internet usage, password protection encryption, viruses?). By doing so, the RCFL is better able to screen, prioritize, and assign the case for examination. Moreover, both the investigator and the Examiner know in advance what is expected of them and can operate accordingly.

Enlighten the Examiner—When submitting digital evidence for examination, investigators should share what they know about the case with the Examiner. While the following suggestions may seem obvious, if this information is not provided to the Examiner early on, delays may result—

- **Inquire About the Owner’s Sophistication Level**—It is helpful for an Examiner to know the equipment owner’s level of sophistication. For instance, a technically advanced owner may have enabled password protection or an encryption application. If an investigator is aware of such tactics or knows the password—this is extremely valuable and timesaving information for the Examiner to have, before beginning the examination.
- **Provide the Names of Suspect(s)/Victim(s)**—Ensure that the Examiner knows the name

of the victim(s) and suspect(s), including nicknames and “chat handles,” along with the specific spellings of these names. Accuracy is absolutely key.

- **Provide a Copy of the Search Authority**—Provide the Examiner with a copy of the search warrant or consent to search so the Examiner knows that there is legal authority to conduct the examination. The search warrant and the affidavit supporting the warrant can also provide valuable information about the investigation and the evidence the investigator is looking for.

Narrow the Examination’s Scope—

Investigators can help an Examiner be more efficient by specifying what they are searching for by providing the following—

- **File Names**—If an investigator is either looking for a particular file, or knows the file’s location, he/she should alert the Examiner—this will save valuable time.
- **Dates**—Is there a specific date range relevant to the investigation? Is the examination limited to certain dates by the search warrant? If the answer is yes to either of these questions, the investigator should let the Examiner know this information.
- **Data Sources**—If multiple computers, media, or hard drives are submitted for examination, state which system or piece of media might have the highest probability of containing the relevant information. For instance, if the Examiner finds evidence on the first system, this may eliminate the need to conduct further examinations on the remaining systems and/or media.
- **Focus the Request**—Focus the request by identifying a particular range of dates, Web sites, user profile(s), or even a downloaded

file(s). By narrowing the search in any one of these areas, the Examiner can fine-tune his/her search.

- **E-Mail Addresses**—A typical computer system contains hundreds, if not thousands, of e-mail addresses—most of which are unrelated to the investigation. To save time, investigators are encouraged to identify the particular e-mail addresses for which the Examiner should search.

Set Time Frames—A quality digital forensics examination may take from 30 to 90 days, sometimes longer, to complete. The time spent is affected by several factors, such as the amount of data that must be reviewed, whether encryption is involved, the user’s level of technical sophistication, etc. Once an Examiner begins work on the case, he/she usually can determine the time frame for the examination and will inform the investigator of this estimate. Conversely, if there is a change in the status of the case and the investigator needs the results sooner than expected—he/she should immediately inform the Examiner.

Remember the RCFL Case

Number—Every case submitted to the RCFL is assigned a case number. Remember that number—the Examiner will use it to provide status updates or preliminary information about the case should the customer request it.

The Final Product—The Examiner will provide his/her findings in the form of a DVD, CD, floppy disk, hard copy, or via a review network. At that point, the Examiner’s work is complete—and the investigator can conduct a full review of the findings. It is important to remember that although most Examiners are investigators by training—they must remain impartial when conducting a digital forensics examination. ■



An imaging room—An Examiner can make exact copies of a computer hard drive, or any other piece of magnetic media, or volatile memory devices such as cellular telephones or PDAs.

“The Uniqueness of Digital Evidence”

In all criminal cases, law enforcement must prove what happened and rely on evidence—whether it’s physical, digital, or circumstantial to support their findings. Digital evidence is unusual because it can play a dual role in a case. Often, it can contain details about what transpired *before* the crime was committed, in addition to valuable clues about the act itself. E-mail exchanges and financial records are classic examples. Another unique characteristic of

digital evidence is that it can be easily tainted or destroyed if not handled properly. Therefore, it is essential that personnel on the front lines have a basic understanding of how to identify and properly preserve digital evidence.

It takes a highly trained specialist to locate digital evidence and make it understandable to an investigator. Although an Examiner cannot absolutely prove who used a particular computer, he/she can provide supporting details such as which user profile or account was in use. It is the investigator’s

responsibility to determine who was “at the controls” when certain events took place.

To help law enforcement better understand and manage digital evidence, the RCFL Program offers a variety of training courses that are taught in each laboratory’s state-of-the-art classroom. Links to these courses are posted on www.rcfl.gov.

Program Accomplishments

FY04 proved to be yet another highly productive year for the RCFL Program. Collectively, RCFL services and support were available to more than 1,400 law enforcement agencies in five states. Program milestones for FY04 included—

Grew the Program—Just one week into FY04, FBI Director Robert S. Mueller, III, announced the selection of five new RCFLs in Buffalo, New York; Houston, Texas; Hamilton, New Jersey; Portland, Oregon; and Salt Lake City, Utah. Soon thereafter, it was announced that Dayton, Ohio; Denver, Colorado; and Philadelphia, Pennsylvania, would each receive an RCFL as well, bringing the total to nine new laboratories. These facilities will greatly enhance the RCFL Program by providing the highest quality digital forensics support to law enforcement agencies across 15 states.

Increased Level of Service—With two more RCFLs in Chicago, Illinois and Kansas City, Missouri, fully operational for the entirety of FY04, the RCFL Program increased its level of service, as indicated by the statistics below—

- Received 1,548 requests for assistance
- Conducted 1,304 forensics examinations
- Participated in 177 search and seizure operations

- Trained 2,040 law enforcement personnel.

Received ASCLD/LAB

Accreditation—In August 2004, the North Texas RCFL (NTRCFL) was accredited by the prestigious American Society of Crime Laboratory Directors/ Laboratory Accreditation Board (ASCLD/LAB)—the first RCFL in the program and the first federally affiliated digital evidence facility to receive this designation in the entire country. The ASCLD/LAB's program is a voluntary initiative in which any crime laboratory can participate to demonstrate that its management, operations, personnel, procedures, and safety procedures meet established standards. The Governor of Texas, FBI Director Mueller, and Attorney General Ashcroft sent their congratulations to NTRCFL Director Michael Morris and his staff, who hail from the Richardson Police Department, Dallas Police Department, the FBI, Garland Police Department, Grand Prairie Police Department, Plano Police Department, Texas Internet Bureau, and the U.S. Attorney's Office—Northern District of Texas.

Supported Several National

Security Cases—Because all RCFL personnel are required to successfully complete the FBI's Computer Analysis Response Team (CART) certification process and to obtain a Top Secret security

clearance, Examiners can work on a variety of investigations from any agency within their designated service area. During FY04, the RCFL Program supported what the U.S. Department of Justice called "...possibly the largest identity fraud case in our nation's history." The case against Scott Levine involved the Acxiom Corporation. He was accused of stealing 8.2 gigabytes (GB) of data from the corporation—causing losses of more than \$7 million. Examiners from each of the RCFLs were part of a team that worked 10-hour days, for five weeks straight, successfully processing more than 100 pieces of evidence. Their findings led investigators to additional subjects and further solidified the Government's case. According to an article posted on CNN, federal agents were "unleashed on the cyber intruders" and made a valuable contribution to the Government's case. All but one of the subjects pled guilty, with one individual still awaiting trial.

In another case, an Examiner on detail to the Chicago RCFL from the Will County Sheriff's Department supported a federal case against a Somali national with ties to Al Qaeda. The suspect was indicted for plotting to blow up a shopping mall in Ohio and is currently awaiting trial. Once the case made national news, the *Star*, an Illinois-based newspaper, wrote, "...when it comes to matters of

In FYO4, articles about the RCFL Program were featured in *Digital Evidence* magazine, and the *Digital Investigator*, an international journal that caters to the digital forensics professionals community.

FYO4 Program Accomplishments at a Glance—

- Accepted 1,548 requests for assistance
- Trained 2,040 law enforcement personnel
- Conducted 1,304 digital forensics examinations
- Was available to approximately 1,400 law enforcement agencies operating in five states
- Participated in 177 search and seizure operations

homeland security, the Will County Sheriff's Department is doing its part by lending one of its officers to help fight terrorism, as well as child pornography and computer fraud."

Both of these cases are excellent examples of how the RCFL Program contributes to protecting our national security while enabling Examiners on detail from state and local police departments to gain valuable digital forensics training and work experience.

Strengthened Ties to Academia—The RCFL Program supports the Digital Forensics Working Group (DFWG), which is composed of representatives from 40 academic institutions and federal, state, and local law enforcement agencies. The group's primary mission is to build academic and research programs in the emerging discipline of cyber forensics. As an active member of the DFWG, the RCFL NPO has

fostered working relationships with a diverse group of stakeholders and is lending its resources to expand the pool of qualified digital forensics professionals.

Supporting Law Enforcement—RCFLs in Action

A primary function of the RCFL Program is to provide technical expertise in support of criminal investigations. During FY04, the program received 1,548 requests for assistance from a

variety of federal, state, and local law enforcement agencies. The following table identifies the top five types of cases for which the RCFL Program provided assistance—

Making an Important Difference...

The RCFL Program receives the greatest number of assistance requests in connection with child pornography investigations. As difficult as these cases are, both personally and professionally, what drives the Examiners is the knowledge that they are helping investigators and prosecutors bring these predators to justice. For example, one case involved the sexual assault on a 15-year-old boy by his neighbor—a former police officer who was suspected of accosting young boys over a 20-year period. Thanks, in part, to two NTRCFL Examiners who found digital evidence on the suspect's computer and later testified in court on their findings, the suspect was found guilty and sentenced to 16 years in prison.

A Not-So-Typical Day in the Life...

North Texas RCFL Examiner Jesse Basham is also a member of the FBI's Hazardous Materials Response Team. It is not often that he wears these two very different hats simultaneously, but such was the case when Examiner Basham helped execute a search warrant at the home of a suspect who may have mailed letters containing anthrax to members of the media and the U.S. Congress.

While still in his hazardous protection suit, Examiner Basham seized five computers and numerous pieces of removable media from the suspect's home, carefully packaging the items for shipment and later examination—a proud first for the RCFL Program.

San Diego

- 1 Child Pornography
- 2 Fraud
- 3 Computer Crimes
- 4 Sexual Offenses/Child Molestation
- 5 Homicide Offenses

North Texas

- 1 Child Pornography
- 2 White Collar Crimes
- 3 Computer Crimes
- 4 Terrorism
- 5 Health Care Fraud

Chicago

- 1 Child Pornography
- 2 Public Corruption
- 3 Copyright Infringement
- 4 Computer Intrusions
- 5 Terrorism

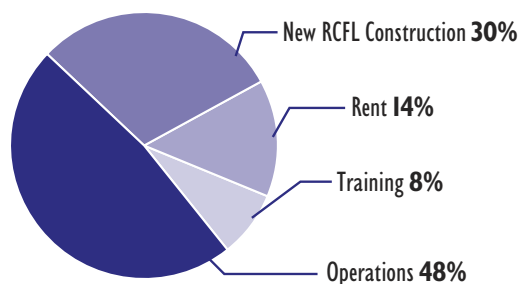
Heart of America

- 1 Child Pornography
- 2 Violent Crime
- 3 Computer Intrusions
- 4 National Security
- 5 White Collar Crime

FY04 Funding

The RCFL Program received \$11 million in Congressional funding for FY04. These funds were used to establish nine additional RCFLs, support the operations of the four existing facilities and the activities performed by the RCFL NPO.

In addition to the funding provided by the Congress, the FBI's Operational Technology Division (OTD), provided \$2.389 million from its own operating funds to support the RCFL Program.



The pie chart above illustrates which activities the program's funds supported during FY04.

Building an RCFL From the Ground Up

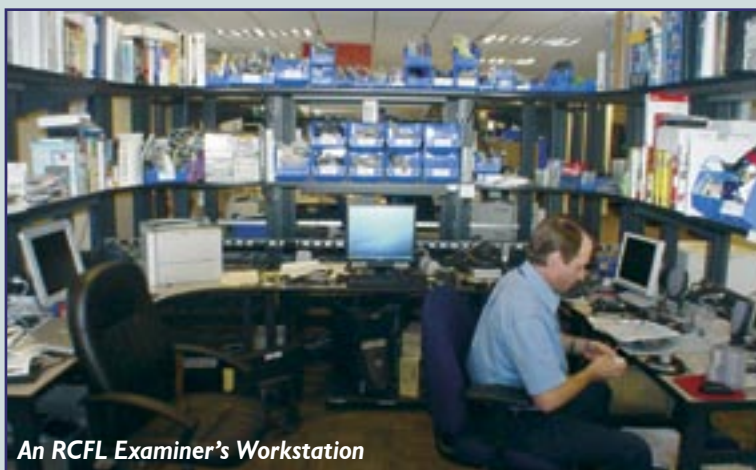
Once an RCFL city is officially selected, the task of building the facility begins. A team, usually headed by a member of the FBI's CART Unit, works with representatives of the RCFL's participating agencies to accomplish the following goals—

- **Select a Location**—Once Congress appropriated funds to the FBI, the RCFL NPO must abide by the rules and regulations concerning the leasing of office space, as set forth by the General Services Administration (GSA). Once the local RCFL team identifies a general area for the RCFL facility, it coordinates closely with the GSA to identify possible sites. The location must have the capacity and flexibility to meet the RCFL's unique specifications regarding security and structural characteristics.
- **Build Out the Facility**—Once a location is selected, the GSA

hires an architect to create a blueprint that meets the RCFL NPO's specific requirements for an RCFL and which recognizes and incorporates the local RCFL team's needs. On average, depending on the space and the amount of construction required, the buildout process can take from two to six months to complete.

- **Procure Equipment and Furniture**—On average, the RCFL Program initially invests an estimated \$26,000

per workstation and updates this equipment approximately every two years at a cost of \$13,000 per unit. An average workstation includes printers, tape drives, digital camera, notebooks, forensic toolkits, and licensed software. Below is a photo of an Examiner's workstation, which often houses up to six examination computers. An RCFL may also engage up to 10 networks in order to process the amount of data associated with its caseload.



An RCFL Examiner's Workstation

Training

Training continues to be one of the most important facets of the RCFL Program, with every facility housing a modern, 20-seat training classroom. Within these classrooms, the program trained 2,040 law enforcement personnel in FY04 regarding:

- Handling of sensitive electronic equipment that becomes evidence
- Computer investigation techniques
- Digital forensics

The RCFL Program is committed to providing valuable digital forensics training opportunities to any law enforcement agency that requests these services—at no cost to that organization. Moreover, the program invests an average of \$9,000 per new Examiner per year for training.

In FY04, 57 current RCFL Examiners received FBI-sponsored training—the same training and certification provided to the FBI's CART Unit.

Moot Court Training

As information is recovered from seized digital evidence, the prosecutor is likely to rely on the Examiner to introduce that evidence into court. As expert witnesses for the prosecution, RCFL Examiners are often required

to testify under oath about how they conducted a forensics examination. To prepare for such situations, Examiners in training participate in “Moot Court,” the final step in the CART certification process. During Moot Court, Examiners practice testifying before real prosecutors and are cross-examined, videotaped, and critiqued.

Moot Court participation is one of the most valuable, realistic training opportunities that the program provides, and its benefits are truly long lasting. For instance, during FY04, an RCFL Examiner testified during the sentencing phase of a child pornography trial, where she provided details about her findings. The jury found the subject guilty, and he received the maximum sentence of 30 years in prison.

“Law enforcement must get a little smarter about computer forensics and digital evidence. If the criminals are learning how to use technology to further their interests, those of us in law enforcement must do the same. We can't afford to wait any longer. The time to start educating ourselves is now.”

—Chief Russ Laine,
Algonquin, Illinois, Police
Department and Member,
National Steering Committee



Students from various law enforcement agencies in northern Illinois receive training at the Chicago RCFL.

“The RCFL Associate Examiner Initiative”

The San Diego RCFL created the Associate Examiner initiative to help former RCFL detailees retain their CART certification. Once Examiners earn this certification, the FBI requires them to take annual CART proficiency tests to maintain it. While an Examiner is detailed to an RCFL, the program schedules and pays for these proficiency tests; however, once an Examiner returns to his/her home agency, he/she may no longer have access to these resources. With the Associate Examiner initiative, former RCFL Examiners can continue their affiliation with the RCFL Program while maintaining their CART certification, and continue to submit their work for peer and administrative review to the RCFL. It's a win-win situation—the program meets its goal of building law enforcement's digital forensics capacity, while Associate Examiners maintain their digital forensics skills.

Image Scan

Many of the cases that the RCFL Program supports involve child pornography or the exploitation of children. To strengthen law enforcement's capabilities in this area, the FBI's CART Unix Program developed a new software tool entitled “Image Scan.” With Image Scan, field investigators can accurately and quickly view a variety of graphical formats on a subject's computer during a consent search—without making any changes to the files. Because of the increased capacity of

computers and other electronic devices, Examiners may need to sift through hundreds—sometimes thousands—of these images. Image Scan accelerates this process while maintaining the forensic integrity of the computer. It is important to note that this tool was not designed to replace a full digital forensics examination in a laboratory environment such as an RCFL.

As the only authorized instructors and distributors for Image Scan outside of FBI Headquarters, each RCFL has a designated Image Scan coordinator on staff who arranges this training for any law enforcement agency in an RCFL's service area that requests it. In FY04, the RCFL Program trained 635 law enforcement personnel in the use of Image Scan.

Law enforcement's response to the Image Scan training has been overwhelmingly positive. Rene Martinez, with the Corpus Christi Police Department, wrote, “Thank you for the opportunity to learn the latest ways of capturing digital images through the Image Scan Software Training.... This is a great asset in our continuing battle against child pornography.”

The RCFL Program often cites



“Image Scan is a highly productive partnership between the RCFL Program and CART. In less than one year, the RCFL staff trained an impressive 635 law enforcement personnel on this software. We will reach even greater heights as we launch new versions of Image Scan in the near future.”

—SSA Dara Sewell
Cart Unit Chief

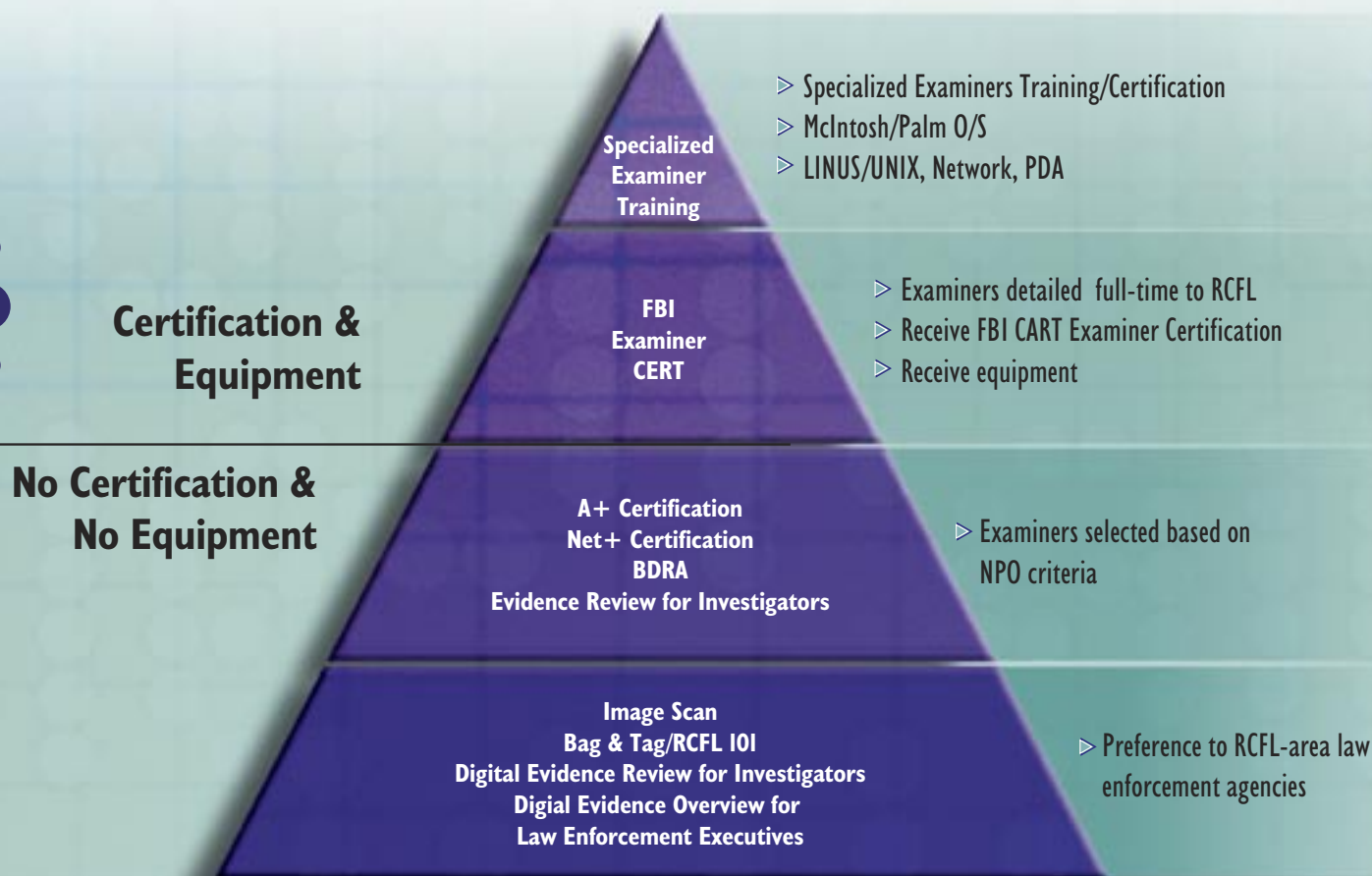
building law enforcement's digital forensics capacity as one of our main objectives. The following statement from Mr. Robert Ener of the Beaumont Police Department, Special Crimes Division, further demonstrates how we are meeting this goal, “The training was excellent. It will assist us in a planned expansion of our sex offender verification checks that will include previewing their computers.”

Basic Data Recovery and Analysis (BDRA)

The National White Collar Crime Control Center (NW3C), a federally funded, nonprofit corporation, developed this 4-1/2 day class, which is available at any

one of the RCFLs and taught by certified instructors. BDRA is a hands-on instruction and discussion about evidence identification and extraction, hardware and software needed to perform a seizure, how to recover erased files, high-tech legal issues, and

more. Any law enforcement official that investigates and prosecutes high-technology crimes, and/or seizes digital evidence, will benefit by taking this course. NW3C's Web site is available at www.nw3c.org/index.html.



There are four tiers to the RCFL Training Pyramid. At the base of the pyramid are the classes offered at RCFLs around the country. These classes: Image Scan, Bag & Tag, Digital Evidence Review for Investigators, and the Digital Evidence Overview for Law Enforcement Executives, form the basis for how investigators in the field react to digital evidence. At the next level are

training classes that are available to law enforcement personnel who want to develop a proficiency in digital forensics. These classes are available to law enforcement personnel through various programs. All of these classes are taught at RCFLs. BDRA and Digital Evidence Review for Investigators are even taught by RCFL NPO instructors. At these two levels, participants do not receive any

equipment or certifications. Classes are offered at various times and are provided free of charge.

At the top of the pyramid are those Examiners who are detailed full-time to RCFLs. They receive FBI CART examiner certification and equipment.

Research, Development, Tool Testing, and Validation

During FY04, the RCFL Program continued to make significant advances in the research and development (R&D) arena. Because RCFLs do not receive a specific budget for R&D, each facility pursues new tools and technologies through a collaborative effort with OTD's CART and Forensic Support Unit (FSU). This exchange of ideas, resources, and personnel benefits all involved as new tools and technologies are created, tested, and then exported for widespread implementation in the field. An example of this collaboration is Image Scan. Although CART created and successfully tested Image Scan, it was the NTRCFL, in conjunction with CART's Unix Program, that designed and developed the training curriculum for users with a nontechnical background. Today, the Image Scan system is available to any law enforcement agency upon request.

Because each RCFL has unique needs and requirements, the R&D agenda for each facility varies. The program achieved the following R&D milestones during FY04—

- **Transportable Storage Area Network**—The NTRCFL first developed the storage area network (SAN) technology to help it better meet its demanding casework needs. A SAN, a single repository that contains data for an individual case, enables an Examiner to

load information more quickly. The NTRCFL took this concept one step further by developing the transportable storage area network (TSAN), which provides the same benefits and advantages of the SAN, but can be brought to any location where evidence is being collected. The TSAN allows Examiners to image 20 servers at a time and allows them to process digital evidence in the field as if they were in a laboratory setting such as an RCFL. Thanks to the SAN and TSAN technologies, cases are being processed more efficiently, and results are being shared more effectively. To date, the CART Unit has purchased more than 26 SANs for the field, and the TSAN technology is successfully being utilized by a number of federal agencies as well.

- **Review Net and Case Agent Review Tool Project**—In conjunction with CART, the NTRCFL developed a tool that enables law enforcement officers to conduct instantaneous key word searches on volumes of processed data, read e-mails, view graphics, and review large amounts of data without modifying or deleting any of the information they see. This project is currently in the testing phase, with the goal of providing this resource to state and local law enforcement agencies.

About OTD...

The FBI's Operational Technology Division (OTD) was created in 2001 and holds full Divisional status. Headed by Assistant Director Kerry E. Haynes, OTD provides the FBI with a wide range of technical services and capabilities, and funds many of the R&D initiatives undertaken by CART and the RCFL Program. OTD's technical expertise plays a key role in every major FBI counterterrorism, criminal investigative, and counterintelligence case, and many of the tools and technologies created and tested by RCFLs, CART and the FSU, and are used by OTD and other law enforcement personnel.



Governance Boards

The RCFL Program established a Governance Board to provide a forum where stakeholders can exchange information, provide advice, have an interactive dialogue, and promote the practice and application of digital forensics within the law enforcement community.

The Governance Boards have two primary outlets—

The National Steering Committee (NSC) is an intergovernmental advisory committee composed of elected government officials or their representatives, and/or employees of federal, state, and local government agencies who have expertise in the science of digital forensics. Half of the NSC membership has legal expertise. The NSC provides advice and makes recommendations to the RCFL NPO and Program's leaders within the FBI and meets on a bi-annual basis.

During FY04, the NSC entered its second year, having successfully made the transition from “forming and storming” to “norming and performing.” The NSC's fall meeting was held on October 10, 2003, at the NTRCFL, and the spring meeting took place on March 25–26, 2004, at the Internal Revenue Service's Computer Crimes Division. During these gatherings, the NSC discussed the following topics—

- **Accreditation**—Although the RCFL NPO supports accreditation for RCFLs, not all NSC members believe that every digital forensics laboratory must have this designation to provide high-quality services. However, with the accreditation of the NTRCFL by ASCLD/LAB, the NSC believes that the RCFL Program should share its knowledge about gaining accreditation with other digital evidence facilities that are managed by other law enforcement agencies.
- **Specialization**—The NSC supports the concept of RCFLs having a specialization in addition to their regular duties. The NSC believes that an RCFL's geographical location may dictate its specialization area and that the need for a certain type of expertise may drive an RCFL to develop a particular skill simply because of demand. If an RCFL develops specific expertise, it should share this knowledge with others in the program. Specialization areas might include embedded computer systems such as appliances; voice communications systems; copy machines; and digital imaging (visual).
- **Customer Support/Training**—During the spring meeting, the NSC elevated customer support/training to the top of its priority list—the issue



being, once a digital forensics examination is completed, does the customer understand what to do with the results? The NSC believes that more assistance is needed in this area, and that the RCFL Program can help by developing more educational tools for such audiences as police departments, judges, prosecutors, and mid-level managers. The goal is to facilitate a better understanding of the field of digital forensics, with a specific focus on seizing evidence, writing search warrants, and identifying and preserving digital evidence and its unique properties.

The RCFL NPO, in conjunction with the RCFLs are considering these

The NSC Team

NSC members represent a diverse group of organizations from across the digital forensics spectrum. In alphabetical order, they include—

Michael Battle	U.S. Attorney for the Western District of New York, member of the U.S. Attorney General's Advisory Committee
Craig Chval	Assistant Attorney General, Missouri Attorney General's Office, member of the National Association of Attorneys General
Benny Del Re	Director, Santa Clara County Crime Laboratory, member of the American Society of Crime Laboratory Directors
Mark Eckenwiler	Deputy Chief, Computer Crime & Intellectual Property Section, U.S. Department of Justice
Jerry Estes	District Attorney, 10th Judicial District, Tennessee, member of the National District Attorneys Association
Russell Laine	Chief, Algonquin Police Department, member of the International Association of Chiefs of Police
Kenneth Laursen	Chief, Major Crimes & Safety, Department of Defense Computer Forensics Laboratory
Douglas A. Schmidtknecht (Co-chair)	Unit Chief, RCFL National Program Office, Federal Bureau of Investigation
Dr. Sujeet Sheno	University of Tulsa, representing the Governor of Oklahoma
Dr. Eugene H. Spafford	Purdue University, Center for Education and Research in Information Assurance and Security (CERIAS), representing the Governor of Indiana
Tony Whitley (Co-chair)	Director, Electronic Crimes Program, Internal Revenue Service

recommendations and how it might implement them in consultation with the NSC.

Local Executive Board (LEB)—

Each RCFL has a corresponding LEB that includes one representative from each of the participating agencies. These boards oversee the operations of the individual RCFL with which they are affiliated, but they do not have any independent legal status.

During FY04, the LEBs affiliated with the San Diego, North Texas, Chicago, and Heart of America RCFLs met regularly to discuss operations and various policy issues concerning their respective RCFLs. Some LEBs also have an educational component where presentations regarding the practice of digital forensics, or new tools and technologies, are given. Each LEB determines how often it will convene, (e.g., monthly

or quarterly), and in between meetings, communicates through updates via e-mail or conference calls.

Also during FY04, several LEBs with newly appointed RCFLs were established and subsequently met throughout the year. These LEBs include the New Jersey, Silicon Valley, Northwest, Intermountain West, Rocky Mountain, and Greater Houston RCFLs.

On the Horizon for FY05

During FY05, the RCFL Program will focus its efforts on achieving the following goals—

- **Obtaining Additional Personnel**—With a demanding caseload before them, the RCFL Directors are under constant pressure to sufficiently staff their facilities to meet both present and future needs. The Directors rely on their participating agencies to send

them qualified personnel to staff the RCFL—a challenging task for these same agencies because they must also contend with the issues of scarce resources and a shortage of qualified personnel. Nonetheless, because of the many benefits associated with RCFL participation, the RCFL NPO is confident that additional law enforcement organizations will become not only customers

but participating agencies. By doing so, this worthwhile investment can produce many returns in both the short and long term.

- **Expand Training Efforts**—To help raise awareness about the value of digital evidence among the law enforcement and legal communities, the RCFL Program is expanding its training initiatives to meet this goal. The program



is also working in partnership with the NSC to offer members of the legal profession various RCFL sponsored training courses. By offering more training opportunities, the program is assisting its colleagues in law enforcement with better understanding such principles as the proper way to handle sensitive electronic equipment, and the role digital evidence plays during a criminal investigation.

- **Requesting ASCLD/LAB Accreditation for Every RCFL**—The NPO requires each RCFL to seek ASCLD/LAB accreditation. During FY05, the San Diego, Chicago, and Heart of America RCFLs are expected to apply for this designation—whereas newly appointed RCFLs are focusing their efforts on launching full operations before taking on this effort.

- **Acquiring Stronger Tools**—All RCFLs face one common challenge—with the increasingly larger storage capacity of electronic devices, there is much more data for Examiners to review. To illustrate this fact, the San Diego RCFL cites the average number of man-hours for each case as approximately 21, with one extremely complex investigation requiring a record 251 man-hours to complete. In light of these circumstances, the RCFL Program is pursuing a number of R&D projects (see R&D section) while also taking the following steps to meet the challenge of increased capacity—

- ▶ **Reviewing a Laboratory Management System (LIMS)**—To better manage and capture important data, the RCFL staff is collaborating on a “requirements needs” document that will help determine whether they should purchase a commercial product or custom design a database to meet its needs.

- **Building Capacity with Finite Resources**—One of the RCFL Program’s guiding principles is to strengthen and build law enforcement’s digital forensics capacity. These resources may take the form of

“It’s not the number of requests—it is the sheer volume of data that is so daunting. One case alone had 12 terabytes of data—compare that to 42 terabytes processed for an entire year. In the very near future, these cases will become the norm—not the exception.”

—Randall L. Bolelli
Director, San Diego RCFL

training, equipment, or technical expertise. On occasion, (and upon request) the RCFL NPO provides technical expertise to those jurisdictions that wish to build a RCFL with non-FBI funds. The RCFL NPO expects this trend to continue as law enforcement’s demand for digital forensics expertise remains strong. Therefore, regardless of budget limitations, the RCFL Program will continue sharing knowledge and advice with our colleagues in law enforcement—because we all share one common goal—to build capacity while operating under the highest standards possible.



PART II—RCFL PROFILES

“By fighting technology with technology, RCFLs are giving law enforcement the edge we need to stay one step ahead of the criminals. We are also aggressively developing and testing new technologies to strengthen our digital forensics abilities. Leveling the playing field isn’t enough—we need to own it.”

—Randall L. Bolelli
Director, San Diego RCFL



Year Established: 1999

Director: Randall L. Bolelli

Service Area: San Diego and Imperial Counties

Internet Address:
www.rcfl.org

Participating Agencies

- California Highway Patrol
- DHS—Immigration and Customs Enforcement
- Escondido Police Department
- Federal Bureau of Investigation
- La Mesa Police Department
- Naval Criminal Investigative Service
- San Diego County District Attorney’s Office
- San Diego Police Department
- San Diego Sheriff’s Department
- U.S. Attorney’s Office—Southern District of California
- U.S. Border Patrol
- U.S. Drug Enforcement Administration
- U.S. Navy, Commander Naval Regional Southwest

PROGRESS & ACCOMPLISHMENTS

During FY04, the San Diego RCFL had several notable accomplishments, including—

- **Increased Output**—The San Diego RCFL increased its output by 19 percent, and processed 42 terabytes of data, compared with 34 terabytes in FY03. This jump in productivity is attributable to an increase in the amount of digital evidence present in each request. With more than 70 local, state, and federal agencies in its service area—the demand for digital forensics services will continue to rise.
- **Established a Formal Local Executive Board**—In May 2004, the San Diego RCFL adopted a new Memorandum of Understanding that served as the legal basis for a formal Local Executive Board (LEB). An LEB is composed of a representative from each of the participating agencies, and their role is to oversee the operations of the RCFL with which they are affiliated.
- **Raised Staffing Levels**—The San Diego RCFL added two new Examiners—raising its staffing level to 20 full-time positions.
- **Welcomed a New Participating Agency**—During FY04, the U.S. Navy, Commander Naval Regional Southwest, joined the San Diego RCFL as a participating agency and assumed its position as a voting member of the LEB.

LOOKING AHEAD

The San Diego RCFL, like its colleagues in the program, is always striving to reduce the average turnaround time for its cases—while simultaneously providing the highest quality digital forensics services possible. To fulfill this formidable and ongoing mandate, RCFL Director Bolelli, along with his LEB, has identified the following goals for FY05—

- **Increase Regional Participation**—The San Diego RCFL plans to boost regional participation to allow for the addition of two full-time Examiners. With a 19 percent increase in its workload in FY04 alone, the San Diego RCFL is optimistic that its colleagues and customers in the local law enforcement community will also share in the operations of the laboratory. In addition, plans are under way to add a full-time evidence custodian position to accommodate the numerous administrative demands.
- **Seek ASCLD/LAB Accreditation**—During FY05, the San Diego RCFL will formally submit an application to ASCLD/LAB for accreditation of its facility.
- **Install a SAN**—To accommodate its burgeoning workload, the San Diego RCFL will install a SAN to enhance all aspects of the laboratory's operations.
- **Expand Service Offerings**—The San Diego RCFL is developing an audio and video analysis component in response to frequent requests for this service from its customers.

STATISTICS FOR FY04

The following tables and charts depict the San Diego RCFL's accomplishments during FY04.

CASEWORK	
Number of service requests	666
Participation in search and seizure operations	106
Number of exams performed	560

CUSTOMER BASE	
Number of federal, state, and local law enforcement agencies in the service area	77

TRAINING	
Number of law enforcement officers trained in various digital forensics, and/or search and seizure techniques	661
Number of detailees who received FBI-sponsored training	17

PERSONNEL	
Total number of detailees	20
New detailees	3
Number of detailees returned to their home agencies	3





"The work we do can make or break a case and may be a factor in deciding whether or not someone goes to jail. With such high stakes, we must do everything we can to submit the best work product possible to the justice system."

—Michael S. Morris
Director, NTRCFL

Year Established: 2000

Director: Michael S. Morris

Service Area: 137 counties
in North Texas

Internet Address:
www.ntrcfl.org

Participating Agencies

- Dallas Police Department
- Federal Bureau of Investigation
- Garland Police Department
- Grand Prairie Police Department
- Plano Police Department
- Richardson Police Department
- Texas Internet Bureau
- U.S. Attorney's Office—Northern District of Texas

PROGRESS & ACCOMPLISHMENTS

FY04 was a pivotal year for the NTRCFL. A list of its noteworthy accomplishments includes—

- **Received Accreditation by ASCLD/LAB**—On August 25, 2004, the NTRCFL achieved a series of "firsts" by becoming the first RCFL in the program, the first federally affiliated digital evidence laboratory, and the first crime laboratory in the State of Texas to become accredited in digital evidence by the prestigious ASCLD/LAB. Overall, this was a very positive experience for the NTRCFL. According to Director Morris, "Now that we have gone through the accreditation process, we all have a better understanding of their policies and procedures, and our customers can have even greater confidence in our work products." The NTRCFL received widespread praise for its efforts, including a proclamation from Texas Governor Rick Perry and a letter of congratulations from Attorney General John Ashcroft. These officials noted the NTRCFL's great accomplishment and praised the staff for "raising the bar of excellence for digital evidence laboratories everywhere."
- **Made Several R&D Breakthroughs**—The NTRCFL played a key role in creating and testing several new technologies. Most notably, it was very involved with both the SAN and TSAN projects. These tools are helping the RCFL and CART Examiners process data more quickly and efficiently, and are giving the

program the edge it needs to address its heavy caseload. The NTRCFL was also integrally involved in the Review Net and Case Agent Review Tool projects. Once implemented, these tools will enable users to conduct a number of different activities (e.g., key word searches, e-mail review, etc.) without altering any of the data they see.

- **Enhanced the Program's Training Offerings**—The NTRCFL, in conjunction with CART, created the training curriculum for the Image Scan technology. In FY04 alone, the RCFL Program trained more than 600 officers on how to use this potent new weapon in the fight against child pornography.

LOOKING AHEAD

The NTRCFL will continue to advance the digital forensics R&D arena, while refining its own service offerings. Specifically, NTRCFL Director Morris, in collaboration with the LEB, has identified the following goals for FY05—

- **Increase Staff Levels**—To help manage its demanding caseload, the NTRCFL hopes to fill three full-time Examiner positions.
- **Reduce Turnaround Time**—The NTRCFL has created several initiatives which, when implemented, will reduce both the administrative and examination requirements for each case.
- **Seek Additional Funding Sources**—To address the increasing costs of doing business, the NTRCFL is pursuing alternative

funding sources, including a state grant.

- **Implement New Tools**—The NTRCFL plans to implement Review Net to enhance operations during FY05.

- **Expand Service Offerings**—The NTRCFL has developed a video analysis component and will begin accepting cases during the second quarter of 2005.

STATISTICS FOR FY04

The following tables and charts depict the RCFL's accomplishments during FY04.

CASEWORK

Number of service requests	350
Participation in search and seizure operations	25
Number of exams performed	342

CUSTOMER BASE

Number of federal, state, and local law enforcement agencies in the service area	573
--	-----

TRAINING

Number of law enforcement officers trained in various digital forensics, and/or search and seizure techniques	500
Number of detailees who received FBI-sponsored training	14

PERSONNEL

Total number of detailees	14
New detailees	3
Number of detailees returned to their home agencies	3

"ASCLD/LAB is the most prominent accrediting body of crime laboratories in the country. Going through the accreditation process was a very positive experience. We all have a better understanding of their policies and procedures, and our customers have even greater confidence in our work products."

—Michael S. Morris
Director, NTRCFL

“The RCFL Program is about partnership and sharing resources. It is through this collaboration that we—the law enforcement community—can significantly enhance our digital forensics capacity. With every officer we train, every examination we conduct, every new technology we develop, we become stronger. Building capacity won’t happen overnight, but rest assured—it is happening. Every RCFL is proof of that.”

—Rick Voss
Director, Chicago RCFL



RCFL

Year Established: 2003

Director: Rick Voss

Service Area: 19 counties in northern Illinois

Internet Address:
www.chicagorcfl.org

Participating Agencies

- Chicago Police Department
- Cook County Sheriff's Office
- Federal Bureau of Investigation
- Kane County Sheriff's Office
- Illinois Attorney General's Office
- Illinois State Police
- Palatine Police Department
- University of Illinois Police Department
- U.S. Drug Enforcement Administration
- Will County Sheriff's Department

PROGRESS & ACCOMPLISHMENTS

FY04 marked the CGRCFL's first full year of operations. During this time, it compiled an impressive track record, which includes—

- **Successfully Completed First Full Year of Operations**—The CGRCFL marked its first full year of operations and welcomed the Kane County Sheriff's Office and the U.S. Drug Enforcement Administration as participating agencies. Subsequently, two full-time Examiners from these agencies joined the CGRCFL's staff.
- **Gained Recognition**—The CGRCFL received two awards for outstanding service in FY04. The first was the Cook County Crime Stoppers Forensics Service Award; and the second was a quality award given by the FBI's CART Unit.
- **Contributed to Several R&D Projects**—The CGRCFL was actively involved in several significant R&D projects including the SAN and TSAN technologies.

LOOKING AHEAD

During FY05, the CGRCFL plans on continuing its momentum and has set the following goals—

- **Augment Services to the Participating Agencies**—During FY05, the CGRCFL will strengthen its offerings to its participating agencies by enhancing the services it provides to them, e.g., increased training opportunities and customized services.

- **Increase the Number of Participating Agencies**—The CGRCFL has set its sights on adding two new participating agencies by the end of FY05. Given the many benefits of RCFL participation, CGRCFL Director Voss and the LEB are confident that this goal is attainable. To increase its ranks, the CGRCFL plans on adding two full-time Examiners by the end of FY05, as well as a systems administrator and an evidence technician.
- **Enhance LEB Participation**—The participating agencies play an important role in the operations of the CGRCFL; therefore, their involvement through meetings and other interactions are vital to the success of the laboratory. To help the LEB members stay engaged in various CGRCFL activities, Director Voss is providing several creative avenues for participation, such as taking votes via e-mail and increasing the involvement of LEB members in Examiner interview panels.
- **Reduce Processing Time**—To decrease the service request backlog and to improve the average processing time per request, the CGRCFL is working on fully implementing several solutions, including increasing the—
 - Availability of SAN space
 - Number of service requests processed on the SAN
 - Number of examination machines
 - Use of review rooms.
 Moreover, the CGRCFL plans on

implementing the new Review Net technology in FY05.

- **Raise Awareness**—The CGRCFL is available to 364 law enforcement agencies in its service area—but not all of these organizations have used or are fully aware of the many services that the laboratory provides. In an effort to raise awareness, the CGRCFL plans to intensify its outreach efforts to local law enforcement and make its Web site more robust by adding additional user-friendly features and training information.
- **Seek ASCLD/LAB Accreditation**—The CGRCFL will seek this accreditation during FY05, but prior to actually doing so, the staff will prepare for this ambitious undertaking by attending an ASCLD/LAB workshop, scheduling weekly ASCLD/LAB planning meetings with the CGRCFL staff, and attending the OTD sponsored ASCLD/LAB inspector training course.
- **Strengthen the CGRCFL's Quality Assurance (QA) Program**—To meet this goal, CGRCFL Director Voss will hold monthly meetings with the quality manager to resolve QA issues, oversee the implementation of an annual QA audit, and establish a quarterly QA award for Examiners by the end of the second quarter.
- **Expand Training Initiatives**—The CGRCFL plans on training an additional 300 law enforcement officers in digital evidence handling and/or Image Scan software by—
 - Working with the North East Metropolitan Regional Training

Center to schedule and publicize, at a minimum, two training sessions per month

- Collaborating with the Mobile Training Units to identify training opportunities for outlying law enforcement agencies in the CGRCFL's service area.

STATISTICS FOR FY04

The following tables and charts depict the CGRCFL's accomplishments during FY04.

CASEWORK

Number of service requests	273
Participation in search and seizure operations	25
Number of exams performed	192

CUSTOMER BASE

Number of federal, state, and local law enforcement agencies in the service area	364
--	-----

TRAINING

Number of law enforcement officers trained in various digital forensics, and/or search and seizure techniques	560
Number of detailees who received FBI-sponsored training	13

PERSONNEL

Total number of detailees	13
New detailees	2
Number of detailees returned to their home agencies	2

"With the RCFL Program, we focus on both the customers and the quality of our work. Are they confident in the results? Will our findings strengthen their case? Are we offering the right services to meet their needs? I believe we are doing all of these things—and more. This program is devising solutions where none existed—that, in itself, is a true innovation."

—Thomas J. Maiorana
Director, Heart of America
RCFL



Year Established: 2003

Director: Thomas J. Maiorana

Service Area: The entire State of Kansas and the western two-thirds of Missouri (total of 171 counties)

Internet Address:
www.harcfl.org

Participating Agencies

- Federal Bureau of Investigation
- Johnson County, Kansas Sheriff's Office
- Kansas Bureau of Investigation
- Kansas City, Kansas Police Department
- Kansas City, Missouri Police Department
- Lawrence, Kansas Police Department
- Lenexa, Kansas Police Department
- Missouri Highway Patrol
- North Kansas City, Missouri Police Department
- Overland Park, Kansas Police Department
- U.S. Attorney's Office—District of Kansas
- U.S. Attorney's Office—Western District of Missouri

PROGRESS & ACCOMPLISHMENTS

During FY04, the HARCFL celebrated its first full year of operations, and during that time, had several laudable accomplishments including—

- **Completed Examiner Certifications**—During FY04, every HARCFL Examiner successfully completed CART training and received his/her certification.
- **Expanded Service Offerings**—The HARCFL received forensic video enhancement equipment and began training its Examiners in its use.
- **Raised Awareness**—The HARCFL has one of the largest service areas in the program—covering almost two states with approximately 800 law enforcement agencies. Therefore, the task of reaching all these agencies is an ongoing challenge. After being featured in the November/December 2004 edition of *Evidence Technology* magazine, the HARCFL sent a comprehensive brochure detailing the HARCFL's services to all 800 of the law enforcement agencies in this service area.
- **Increased the Number of Participating Agencies**—The HARCFL welcomed the North Kansas City, Missouri Police Department to its ranks—raising the number of participating agencies to 12.
- **Enhanced Efficiency**—The basic SAN infrastructure was completed. In addition, a client/server model

was installed at each Examiner's workstation to increase the performance and efficiency of forensic processing.

LOOKING AHEAD

Now that the HARCFL is firmly established in both the Missouri and Kansas law enforcement communities, HARCFL Director Maiorana, in consultation with his LEB, has identified the following goals for FY05—

- **Develop Additional Training Courses**—Training continues to be one of the most popular and sought-after offerings of the RCFL Program. The HARCFL is no exception and is working on developing several new training courses to add to its curriculum. These courses, once completed, will be exported for use throughout the RCFL Program.
- **Increase the Number of Training Classes**—With thousands of law enforcement officers in its service area, the HARCFL plans on offering more frequent training sessions, including the popular Image Scan, for area law enforcement personnel.
- **Apply for ASCLD/LAB Accreditation**—The HARCFL will seek this accreditation during FY05 and will work with its counterparts in the program to adequately prepare for this designation.
- **Implement Review Net**—Although this new technology is still in the testing phase, the HARCFL, along with others in the program, plans on implementing this tool during FY05 to increase efficiency.

- **Fully Incorporate Video Enhancement**—During FY04, the HARCFL staff received, and began training on sophisticated video equipment. During FY05, they plan to offer video enhancement to HARCFL customers.

- **Decrease Request Turnaround Time**—With the incorporation of powerful new technologies and tools, the HARCFL is confident that it will decrease request turnaround time—while improving the quality of its forensics examinations.

STATISTICS FOR FY04

The following tables and charts depict the RCFL's accomplishments during FY04.

CASEWORK

Number of service requests	259
Participation in search and seizure operations	21
Number of exams performed	210

CUSTOMER BASE

Number of federal, state, and local law enforcement agencies in the service area	800
--	-----

TRAINING

Number of law enforcement officers trained in various digital forensics, and/or search and seizure techniques	319
Number of detailees who received FBI-sponsored training	13

PERSONNEL

Total number of detailees	13
---------------------------	----

Acknowledgements

The RCFL National Program Office would like to thank FBI Director Robert S. Mueller, III, and Assistant Director Kerry E. Haynes, Operational Technology Division, for their steadfast and tireless support throughout the year.

We also wish to thank the RCFL Directors and staff, CART, FSU, the NSC, and the LEB chairs, including SAC Roderick L. Beverly, SAC Daniel R. Dzwilewski, ASAC Sherry Fleming, ASAC Kevin Fryslie, SAC Mark Mershon, SAC Kevin L. Stafford, ASAC Joseph C. Ways, Sr., and Richardson Police Chief Larry Zacharias, for their unwavering dedication and commitment to the program.

In addition to the above mentioned individuals and offices, the RCFL NPO thanks our colleagues in the following FBI Field Divisions for aiding the RCFL mission throughout the year by generously their sharing valuable resources and time with us—



- FBI Buffalo Field Division
- FBI Chicago Field Division
- FBI Cincinnati Field Division
- FBI Dallas Field Division
- FBI Denver Field Division
- FBI Houston Field Division
- FBI Kansas Field Division
- FBI Newark Field Division
- FBI Philadelphia Field Division
- FBI Portland Field Division
- FBI Salt Lake City Field Division
- FBI San Diego Field Division
- FBI San Francisco Field Division

Finally, a special thanks goes to the following participating agencies who compose and are at the heart of the RCFL Program—

- California Highway Patrol
- Chicago Police Department
- Cook County Sheriff's Office
- Dallas Police Department
- DHS—Immigration and Customs Enforcement
- Escondido Police Department
- Federal Bureau of Investigation
- Garland Police Department
- Grand Prairie Police Department
- Illinois Attorney General's Office
- Illinois State Police
- Kane County Sheriff's Office

- La Mesa Police Department
- Missouri Highway Patrol
- Naval Criminal Investigative Service
- North Kansas City, Missouri Police Department
- Overland Park, Kansas Police Department
- Palatine Police Department
- Plano Police Department
- Richardson Police Department
- San Diego Country District Attorney's Office
- San Diego Police Department
- San Diego Sheriff's Department
- Texas Internet Bureau
- U.S. Attorneys Office—
 - District of Kansas
 - Northern District of Texas
 - Southern District of California
 - Western District of Missouri
- U.S. Border Patrol
- U.S. Drug Enforcement Administration
- U.S. Navy, Commander Naval Regional Southwest
- University of Illinois Police Department
- Will County Sheriff's Department

**“The RCFL Program—
America’s Premier
Computer Forensics
Laboratory Network”**

Engineering Research Facility
Building 27958-A
Quantico, VA 22135
Attn: ERF Annex
RCFL National Program Office

Telephone: 703-902-5502
Internet: www.rcfl.gov
E-mail: info@nationalrcfl.org



REGIONAL COMPUTER
FORENSICS LABORATORY
NATIONAL PROGRAM OFFICE