



REGIONAL COMPUTER
FORENSIC LABORATORY

REGIONAL COMPUTER
FORENSIC LABORATORY
PROGRAM

FISCAL YEAR 2003
ANNUAL REPORT

FOREWORD

Fiscal Year (FY) 2003 was an exciting and very productive time for the Regional Computer Forensic Laboratory (RCFL) Program. During FY 2003, we opened two RCFLs in Kansas City and Chicago. With the selection of five additional sites, the Program has become the premier computer forensics laboratory network in the country, literally doubling in size, while providing the highest quality computer forensics services available to law enforcement.

Because the RCFL Program is relatively young, it has been extremely gratifying to watch this initiative evolve and flourish. Thanks to the support of the U.S. Congress, the FBI leadership, and most importantly, the many law enforcement and government agencies at the state, local and Federal levels who are at the heart of this Program; we are fulfilling our mission of strengthening computer forensics capacity and quality, to deliver trusted results.

This is the inaugural edition of the RCFL Program's Annual Report. We hope this publication gives our stakeholders a better understanding of what computer forensics is; why there is such a need for this expertise, especially post 9/11; and how law enforcement agencies at all levels are applying this science to find digital evidence that can help prosecutors secure a conviction in a court of law.

The use of electronic equipment to facilitate crime is a growing and troubling trend that must be countered by law enforcement through ingenuity, innovation and partnership. By leveraging our scarce resources, the law enforcement community can—and will put a halt to this phenomenon. In the interim, there is admittedly much more to do in this area, but we are unequivocally on the right track with this Program.

Douglas A. Schmidtknecht
Unit Chief
RCFL National Program Office

TABLE OF CONTENTS

PART I: PROGRAM OVERVIEW	2
INTRODUCTION	2
RCFL SERVICES	3
SITE SELECTION	4
FY 2003 FUNDING.....	6
PROGRAM ACCOMPLISHMENTS	7
RCFLs IN ACTION.....	9
TRAINING.....	11
RESEARCH & DEVELOPMENT	12
PARTNERSHIPS AND OUTREACH	13
CHALLENGES AHEAD	15
 PART II: RCFL PROFILES	 17
SAN DIEGO RCFL	18
NORTH TEXAS RCFL	22
CHICAGO RCFL.....	26
HEART OF AMERICA RCFL.....	30
 ACKNOWLEDGEMENTS.....	 35

INTRODUCTION

Comparatively speaking, computer forensics is a fairly new discipline that is defined as “the application of science and engineering to the problem of digital evidence.” Digital evidence may be extracted from any type of electronic equipment, such as a computer, a personal digital assistant, a digital camera or a cell phone.

Because of the wide availability and easy access to electronic equipment, criminals have gone “high-tech” and are using these resources to enhance and maintain their illegal enterprises. As a result, traditional offenses such as financial and commercial crimes are becoming automated, complete with coded records and encrypted data. Given this new reality, law enforcement has had to become just as resourceful by creating initiatives such as the RCFL Program, where law enforcement is leveraging technology to comprehend digital evidence.

In 1999, a coalition of law enforcement agencies pooled their personnel and funding resources to open the first FBI sponsored computer forensics laboratory in San Diego. This became the starting point for what has now become a national, FBI sponsored computer forensics laboratory program.

Although RCFLs were operating in San Diego and North Texas before the events surrounding 9/11, their valuable expertise became all the more evident during this period of our Nation’s history. Several RCFL Examiners supported the Pentagon bombing investigation, working around the clock to examine the computers used by the terrorists. During these critical investigations, Examiners assigned to the North Texas and San Diego RCFLs provided the FBI with much needed results in record time.

“The RCFL Program is a critical component in our efforts to support state and local law enforcement agencies nationwide. By combining the extraordinary talents and resources of law enforcement agencies at all levels, our ability to investigate criminals and detect and prevent acts of terrorism becomes considerably more robust.”

—FBI Director
Robert S. Mueller III



An RCFL is a single-service computer forensic 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

“COMPUTER FORENSICS VS. CYBERCRIME”

More often than not, there is a misperception that computer forensics and cybercrime investigations are one and the same. Not so. The two are really quite different, from their applications, purpose, and end results. A cybercrime may involve a range of offenses from copyright infringement, computer intrusions, hacking, Internet fraud, theft of trade secrets, child pornography/exploitation, to Internet harassment, etc. Cybercrime investigators must find the perpetrators responsible for such acts and assemble enough evidence to charge them with the crime.

Computer forensics professionals do not conduct investigations, rather, their job is to find and decipher digital evidence that may be located on any type of electronic equipment such as a computer, cell phone, pager or fax. The job of interpreting the evidence falls to the investigator and the prosecutors, not to the computer forensic Examiners. Their impartiality and objectivity are very important and lend credibility to the Examiners' findings in court.

SITE SELECTION

The RCFL selection process is a pragmatic, step-by-step approach that was designed to establish these facilities not only in places where they are needed most, but also in jurisdictions that are most capable of supporting the laboratory for the long term. The following steps give a brief overview, from start to finish, of how the National Program Office (NPO) works in partnership with their law enforcement counterparts to select and establish an RCFL:

STEP #1: FUNDING

RCFLs receive their operating budgets primarily through Federal funds appropriated by the U.S. Congress; these funds are managed by the FBI's Investigative Technology Division (ITD).

STEP #2: PROPOSAL SOLICITATION

Once Federal funds are made available to establish an RCFL, the NPO works with the FBI Field Offices to solicit proposals from interested law enforcement coalitions.

STEP #3: PROPOSAL EVALUATION & SUCCESS FACTORS

The NPO carefully evaluates each proposal submitted by FBI Field Offices using specific factors that predict successful RCFL performance. Based on past experience, these factors include the existence of:

- Strong community-wide support for an RCFL
- Strong demand for computer forensic examination services in a region

"The real benefit to local law enforcement is none of us, especially small and mid-size departments, can afford this kind of facility or the personnel. It's a matter of money; we can't do it on our own."

—Bill Pross, Independence, Missouri
Police Department Spokesman

- A commitment to securing a qualified director and staff
- A large pool of available and qualified talent who will be trained and certified as Forensic Examiners
- An easily accessible location

STEP #4: SELECTION CRITERIA

Once the NPO completes their evaluation of the proposals, they narrow the field down to those applicants who most closely adhere to the predictors for successful RCFL performance. This is when the site selection phase begins. During this phase, representatives of the NPO personally meet with each candidate and their partner agencies to ascertain their ability and readiness to operate an RCFL.

STEP #5: SITE SELECTION

The evaluation team prepares a report for the FBI Director that summarizes their findings. The FBI Director makes the final site selection, and once this decision is made, the NPO notifies the various FBI Field Offices and their partner agencies.

STEP #6: IMPLEMENTATION

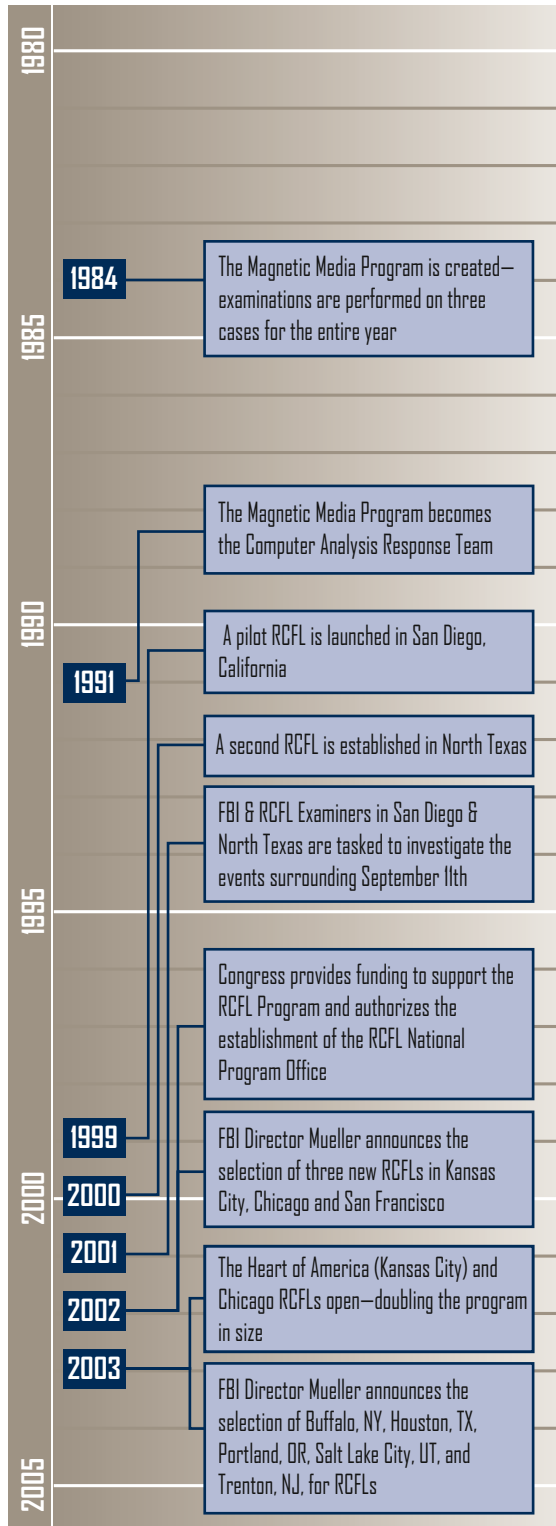
The implementation phase encompasses all the activities required to get an RCFL up and running. Cooperation and collaboration among different law enforcement agencies are key during this period. Typically, the major planning activities include:

- Coordinating the Memorandums of Understanding between the FBI and each Participating Agency;
- Evaluating and meeting with potential computer forensic Examiners;
- Creating individualized training programs for every Examiner to begin the certification process;
- Securing space and equipment for the RCFL;
- Conducting outreach activities with law enforcement agencies in the RCFL's service area.

STEP #7: STAND-UP

Once the implementation phase is completed, and the RCFL officially opens for business, the laboratory begins accepting requests for computer forensic support from any law enforcement agency in its service area.

The Evolution of Computer Forensics Within the FBI



RCFLs are a modest investment with a high rate of return. During FY 2003, Congress appropriated \$7.2 million for the RCFL Program. These funds were used in part to open two new RCFLs, and paid for the acquisition, build-out, and lease of laboratory space, furniture, computer equipment and technical training for the detailees in these labs. The funds were also used to support the efforts of the NPO, and to supplement the continued operations of the San Diego RCFL, whose facility was expanded, and the North Texas RCFL, which moved into a larger facility.

"They're putting in first-rate equipment, and it will be more advanced than what we have. Everyone needs access to collaboration like this."

—Sgt David Hudspeth
Chicago Police Department

PROGRAM ACCOMPLISHMENTS

The RCFL Program achieved several significant milestones in FY 2003. FBI Director Mueller lauded the Program, calling it “a critical component in our efforts to support state and local law enforcement agencies nationwide.” For FY 2003, highlights and noteworthy accomplishments for the Program included:

- **Opened two RCFLs**

The Chicago RCFL opened in March and is serving nineteen counties throughout the Chicago area. The Kansas City area also welcomed its first computer forensics laboratory when the Heart of America RCFL opened in July. The Missouri based facility serves the entire state of Kansas and the western two-thirds of Missouri.

- **Provided Valuable Expertise**

RCFLs are providing much needed computer forensic expertise to law enforcement agencies that lack such resources.

This situation is especially prevalent in smaller departments; however, the same scenario is common among larger organizations. In FY 2003, the RCFLs in San Diego, Dallas, Chicago, and Kansas City offered their resources to hundreds of law enforcement organizations in 372 counties in their collective service areas. This number will increase in FY 2004 as additional RCFLs become operational.

In FY 2003, the RCFL Program processed 82.3 terabytes of data. To visualize this, consider that 82.3 terabytes is the equivalent of roughly 3,427,644 boxes of paper filled with text.

- **Strengthened Capabilities**

During FY 2003, the San Diego RCFL reduced its processing time, with 89% of the examination requests completed in 90 days or less, compared with 81% for the previ-



ous year. The North Texas RCFL also moved into a larger facility that can accommodate up to twenty-three Examiners.

- **Participated in 196 Search and Seizure Operations**

In FY 2003, RCFL Examiners participated in 196 search and seizure operations.

- **Built Computer Forensic Capacity in Regions Across the U.S.**

In FY 2003, approximately 56 detailees participated in the RCFL program. Six Examiners completed their assignments with the North Texas and San Diego RCFLs and returned to their home agencies, bringing a wealth of experience and highly coveted technical skills back with them.

- **Launched the National Steering Committee**

The RCFL Program is very interested in sharing and exchanging ideas and information about the Program with key stakeholders, and convened the National Steering Committee (NSC) to meet this objective. The NSC, an intergovernmental advisory committee, met on April 1, 2003, and in June of the same year.

RCFL ACCOMPLISHMENTS AT A GLANCE:

- ✓ Accepted 1,444 requests for service
- ✓ Participated in 196 search and seizure operations
- ✓ Trained 1,541 law enforcement personnel
- ✓ Conducted 987 computer forensic examinations
- ✓ Served law enforcement agencies operating in 372 counties spanning five states



In FY 2003, the RCFL Program processed 82.3 terabytes of data.

During FY 2003, the RCFLs supported a wide variety of cases ranging from acts of terrorism, homicide, and sexual assault, to white-collar crimes, such as computer intrusion and identity theft. Many of the cases supported by the RCFL Program involve child pornography or the exploitation of children. While this is disturbing, the Program's Examiners are applying their skills to locate digital evidence that can secure convictions in court.

"Where we used to look at a homicide suspect's letters, now it's evolved into an electronic format. This is a quickly growing situation and law enforcement needs to pool its resources to face it."

—Mark Mershon
Special Agent in Charge,
FBI San Francisco Field Office

CASE CLOSED

The North Texas RCFL supported a Federal case that involved the examination of a computer owned by a suspect who was a first grade teacher and a youth pastor. Once the Examiners found child pornography on the subject's computer, the defendant admitted to molesting four minor children. In another case, the NTRCFL successfully defeated the password on four password protected zip disks. The Examiner then found evidence of child pornography, and provided this information to the investigator on the case.

The following tables list the top five types of cases supported by the RCFL Program during FY 2003:

San Diego

- 1 Fraud
- 2 Child Pornography
- 3 Computer Crimes
- 4 Sex Offenses
- 5 Homicides

Chicago

- 1 Child Pornography
- 2 Fraud
- 3 Corruption of State/Local Officials
- 4 Computer Intrusions
- 5 Copyright Infringement

North Texas

- 1 Child Pornography
- 2 Terrorism
- 3 Computer Intrusions
- 4 Forgery
- 5 Criminal Solicitation of a Minor

Heart of America

- 1 Crimes Against Children/Child Pornography
- 2 Computer Intrusions
- 3 White Collar Crimes
- 4 Violent Crimes
- 5 Counterintelligence/Counter terrorism

TRAINING

Training is a cornerstone of the RCFL National Program, and as such, is one of the most sought after, highly regarded benefits of participation. This training takes two forms: training law enforcement personnel in a region, and training individuals detailed as Examiners to the RCFLs.

TRAINING LAW ENFORCEMENT OFFICERS IN A REGION

As part of their service offerings, the RCFLs train law enforcement personnel in their service area regarding:

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

In FY 2003, the RCFL Program trained 1,541 law enforcement officers in these techniques. That number is expected to rise in FY 2004 as the RCFL Program continues to grow.

TRAINING RCFL PERSONNEL

RCFL Examiners receive the same training and certification that is provided to the FBI's Computer Analysis Response Team (CART) certified Examiners. RCFL Examiners are not employees of the lab, rather they are considered "detailees" from the Participating Agencies. Many RCFL Examiners cite the opportunity to obtain the prestigious CART certification as one of the greatest benefits of joining the Program. Certification may take up to a year, and during that time an Examiner trainee receives an individualized training program that takes into account his/her past work experience. He/she will also take as much as six

weeks of classroom training while undergoing extensive on-the-job-coaching. Training begins as soon as possible, sometimes even before a new laboratory opens. Those who already have a background in computer forensics need about six to nine months before they can fully assume an Examiner's duties.

An Examiner trainee must obtain CART certification before he/she may conduct examinations independently.

In FY 2003, approximately 56 detailees received FBI sponsored computer forensics training. The Chicago RCFL reported that one Examiner received their CART certification, while six Examiners received 80% of the required training needed to obtain this certification.

In 2003, 56 RCFL detailees received FBI sponsored computer forensics training. Six Examiners returned to their home agencies, further building computer forensics capacity in the San Diego and North Texas regions.

"In just one year, the RCFL staff trained over fifteen hundred law enforcement officers. The benefits of having a knowledgeable workforce in computer forensics are immeasurable. As more officers are trained in these techniques, the better we will be in preserving digital evidence that can be used to convict a child pornographer, a terrorist, and anyone else who uses technology to facilitate a crime. "

—Marcus Thomas,
Deputy Assistant Director
Investigative Technology Division

RESEARCH & DEVELOPMENT

Each RCFL has a number of activities and services it performs, with research and development being one of them. Because the RCFLs are based in diverse geographical locations, each has unique needs and is pursuing different technologies to meet its specific requirements. Once a technology is sufficiently tested and approved, the application is recommended for use by all of the laboratories in the Program. During FY 2003, the RCFL Program achieved the following accomplishments in the research and development arena:

Write Block Technology—The San Diego RCFL tested the write blocker technology that allows the user to read all the files on a computer's hard drive without the risk of damaging or altering any of the stored information. Today, every RCFL and the FBI's CART are applying this technology with great success.

Storage Area Network (SAN)—In response to meeting their demanding casework needs, the North Texas RCFL took the initiative to develop an array of new technologies, one of which is the SAN or storage area network. A SAN is a single repository that contains data for an individual case, and enables an Examiner to load information more quickly. After being sufficiently tested in FY 2003, the SAN technology was exported to other RCFLs throughout the Program as well as the FBI.

The write blocker and SAN technologies all reflect the collaborative spirit of the RCFL Program. By taking the lead in developing new technologies to meet the challenges before them, the RCFL Program is developing new tools that benefit not only the laboratories in the Program, but also all of law enforcement. The RCFL Program will continue to develop and test new technologies in FY 2004 and beyond.



PARTNERSHIPS AND OUTREACH

The RCFL Program attributes much of its success to the working relationships between the FBI and a range of law enforcement personnel from all levels of government. By initiating and cultivating partnerships, gathering feedback, and soliciting new ideas, the FBI has grown and will continue to advance the Program.

The creation of the RCFL Governance Board initiative underscores the importance of partnership and outreach. Under this initiative, local stakeholders play a role in overseeing the operations of their local RCFLs. National stakeholders have also been given a platform to furnish expert ideas and diverse opinions regarding computer forensics and the RCFL Program. Descriptions of the two types of Governance Boards follow:

- **Local Executive Board**—Each RCFL has a corresponding Local Executive Board that includes one representative from each of the Participating Agencies. These Boards oversee the day-to-day operations of the individual RCFL with which they are affiliated, but they do not have any independent legal status. In FY 2003, the Heart of America and Chicago RCFLs hosted several Local Executive Board meetings, joining their counterparts in San Diego and North Texas.
- **National Steering Committee**—During FY 2003, the Program achieved a major milestone when it successfully launched the NSC. The 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 computer fo-

rensis. The mission statement devised by the NSC is as follows:

The NSC works with the NPO to contribute to the sustained development of the RCFL Program. The NSC provides expert guidance for the advancement of RCFLs, and fosters awareness by communicating the benefits and challenges of the RCFL Program.

NSC ACCOMPLISHMENTS FOR FY 2003

The NSC had a productive first year. Initially, the group devised and agreed on operating procedures and selected Tony Whitledge, Director of the Internal Revenue Service's Electronic Crimes Program, to serve as the NSC's co-chair, along with the NPO Director.

The NSC also selected their priorities and is working on developing recommendations regarding these issues:

1. Enhance awareness about the RCFL Program
2. Grow the Program
3. Promote quality

"This is a very exciting development for RCFLs and the science of computer forensics. Because the NSC has brought together experts in computer science and security, forensic science, prosecutors and law enforcement, we are positioned to make an immediate and meaningful contribution to the RCFL Program."

—Tony Whitledge
NSC Co-chair

MEET THE NSC MEMBERS

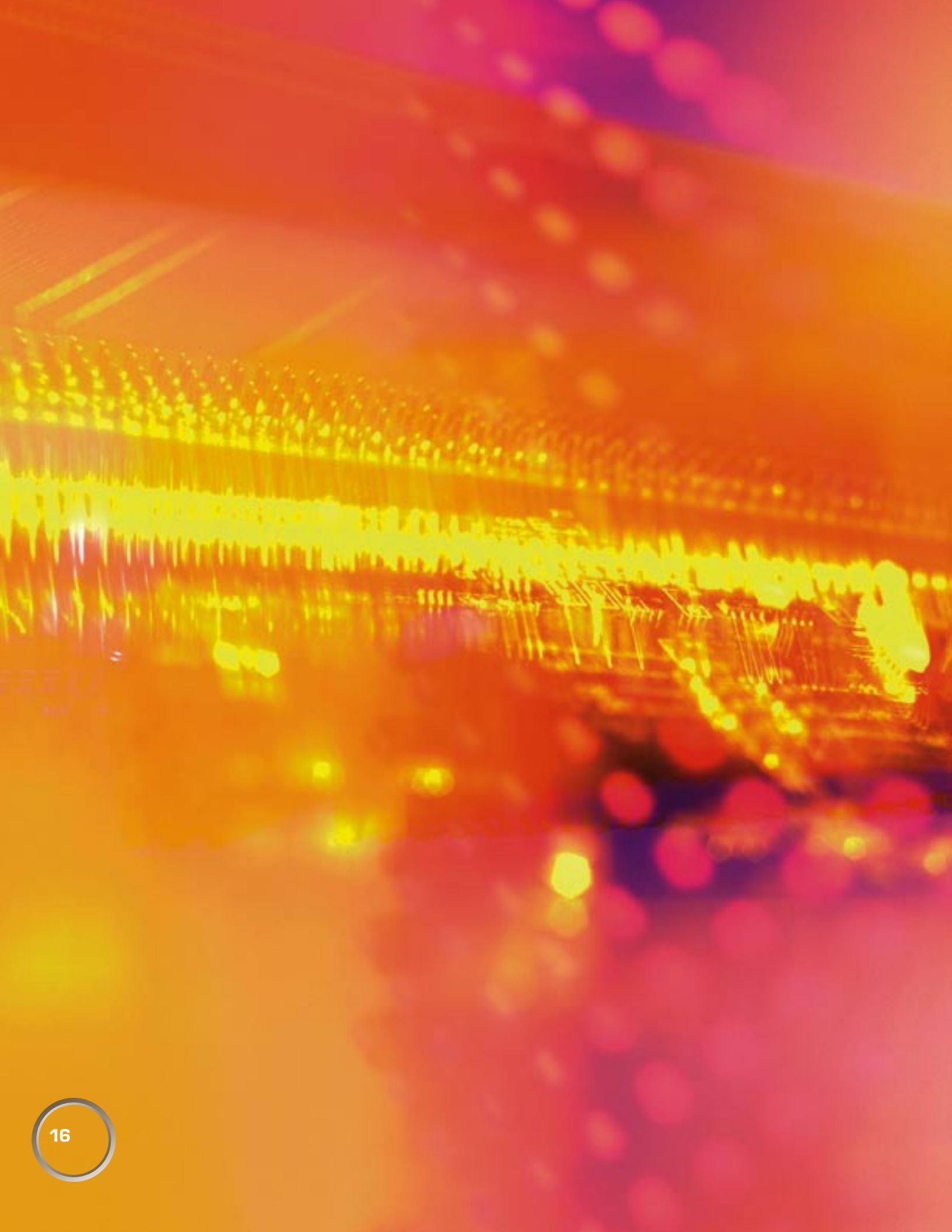
The NSC members hail from a diverse group of organizations from across the computer forensics spectrum. In alphabetical order, they are:

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 General, 10th Judicial District, Tennessee, member of the National District Attorneys Association
Aaron Kennard	Sheriff of Salt Lake City County, Utah, member of the National Sheriffs 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 Forensic Laboratory
Douglas A. Schmidtknecht	Co-chair, Director, RCFL National Program Office, Federal Bureau of Investigation
Dr. Sujeet Sheno	University of Tulsa, representing the Governor of Oklahoma
Professor Eugene H. Spafford	Purdue University CERIAS, representing the Governor of Indiana
Tony Whitledge	Co-chair, Director, Electronic Crimes Program, Internal Revenue Service

CHALLENGES AHEAD

The RCFL Program identified several goals aimed at strengthening and enhancing the Program during FY 2004. They are as follows:

- **Grow the Program While Maintaining Quality**—In FY 2003, FBI Director Mueller selected five new locations in diverse geographical locations to receive RCFLs. The NPO, in coordination with the representatives of each new RCFL, is establishing a standardized set of procedures, quality controls, and processes for each facility. This ensures that each RCFL is providing the highest quality computer forensic services available to law enforcement.
- **Obtain American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) accreditation for every RCFL**—Although all RCFLs currently adhere to strict guidelines and protocols, FBI leadership believes that accreditation will enhance and strengthen the quality of the RCFLs services. The North Texas RCFL will be the first to submit an application and will undergo the accreditation process in FY 2004, with the remaining RCFLs following suit. ASCLD/LAB accreditation in the digital evidence discipline is a new offering; therefore, as each RCFL becomes accredited, it will share its knowledge and experience with others in the Program.
- **Continue to Raise Awareness**—Because computer forensics is an evolving and growing science, raising awareness among the law enforcement and legal communities about its existence is a constant goal for the Program. The RCFLs are meeting this challenge by training law enforcement personnel, working closely with the NSC to reach key interest groups, and educating an array of stakeholders about RCFLs and the field of computer forensics.
- **Increase Agency Participation**—In FY 2003, a total of thirty-eight law enforcement agencies participated in the RCFL Program. In order to keep pace with the casework, each RCFL must maintain and recruit qualified personnel. (The North Texas RCFL projects a 20% increase in casework alone in FY 2004.) In FY 2004 and beyond, the RCFL Program is committed to increasing the number of Participating Agencies because they are responsible for detailing the personnel to work in the laboratories.
- **Continue Addressing Data Growth**—The rapid growth in the volume of data associated with each examination is a major challenge before the Program. For example, a Personal Digital Assistant (PDA) on the market today has the same, if not more storage space than the average desktop computer had just a few years ago. Given the increased storage capacity of electronic equipment like PDAs and computers, Examiners simply have more to review—making investigations more complex and time consuming. The RCFLs are ready to meet the challenge though, through training, by applying new techniques for rapidly imaging electronic media, and by using the latest, most sophisticated equipment and technology.



PART II: RCFL PROFILES

Part II of this report focuses on the individual RCFLs that are currently operating in San Diego, California; Dallas, Texas; Chicago, Illinois; and Kansas City, Missouri. Given their different geographical locations, each of these RCFLs is successfully managing its own set of unique challenges and caseloads. However, they all share a deep commitment to providing first-rate computer forensic services to area law enforcement, and to continuously developing their skills through training and involvement in cases that offer once in a lifetime opportunities to learn and grow. RCFL Examiners cite these experiences as one of the most gratifying and valuable aspects of the job.

Each of these profiles features the Participating Agencies for the RCFL, whose role is to provide personnel and resources for the purpose of operating the laboratory. Their willingness to join this national crime-fighting initiative is absolutely vital to the continuing success of the RCFL Program.

As these individual profiles demonstrate, the partnerships and working relationships that serve as the foundation for the RCFL Program are truly having a tangible and positive impact on the local level—and for the Nation as a whole.



SAN DIEGO RCFL

Year Established

1999

Director

Randall A. Bolleli

Service Area

San Diego and Imperial Counties

Internet Address

www.rcfl.org/

PARTICIPATING AGENCIES

- California Highway Patrol
- Chula Vista Police Department
- 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. Border Patrol
- U.S. Attorney's Office
- U.S. Drug Enforcement Agency

"One of the biggest challenges facing law enforcement today is technology - and the key ingredient to meeting this challenge is the highly qualified men and women assigned to the RCFLs."

—Randall L. Bolelli, Director
San Diego RCFL

INTRODUCTION

The San Diego RCFL has the distinction of being the first FBI sponsored RCFL. While being first makes them somewhat unique, the situation facing the San Diego law enforcement community was all too common: demand for computer forensic services far outweighed the supply. The situation needed improvement, and area law enforcement was determined to do something about it. The FBI's San Diego Field Office, along with several other local law enforcement agencies, decided to pool their resources to establish a computer forensics laboratory. The FBI assumed a majority of the start-up costs, while the other Participating Agencies donated personnel to staff the new lab. The concept worked. In a short while, the San Diego RCFL established a clear standard for the effective and efficient examination of digital evidence. Working as a team, the men and women assigned to the lab began examining digital evidence and were able to address the computer forensic needs of law enforcement in San Diego in a way that had never been done before.

PROGRESS & ACCOMPLISHMENTS

Today, the San Diego RCFL is an established entity and a respected member of the area's law enforcement community. With over forty law enforcement agencies in its service area, the San Diego RCFL received 707 requests for service in FY 2003, which involved approximately 34 terabytes of data. Of those requests, they performed 590 examinations and participated in 117 search and seizure operations.

Even with an increasing caseload, the San Diego RCFL continues to place great importance on supporting investigations in a more

timely and efficient manner. In FY 2003, the San Diego RCFL made several operational enhancements, which resulted in a reduction in its average processing time of service requests. Specifically, eighty-nine percent of the service requests were completed in 90 days or less, compared with 81% for the previous year.

Another highlight for FY 2003 was the addition of a full-time network engineer. This position was established to better manage and maintain all internal computer systems and networks, and to improve the operational workflow of the lab. By having a full-time network engineer on staff, the lab was able to dedicate more resources to research and development efforts. As a result, this strengthened the staff's ability to address constantly changing technologies, and enhanced their overall capability and performance during FY 2003.

CHALLENGES AHEAD

During FY 2004, the San Diego RCFL will have marked its fifth anniversary. Director Bolelli remains committed to ensuring a continuously high level of quality control and efficiency for the lab.

Specific goals for FY 2004 include:

- Increasing regional participation to a level that includes at least twenty computer Forensic Examiners.
- Establishing a more formalized Local Executive Board
- Implementing an automated Evidence Tracking and Case Management System
- Exploring nationally recognized laboratory accreditation and/or certifications for the San Diego RCFL.

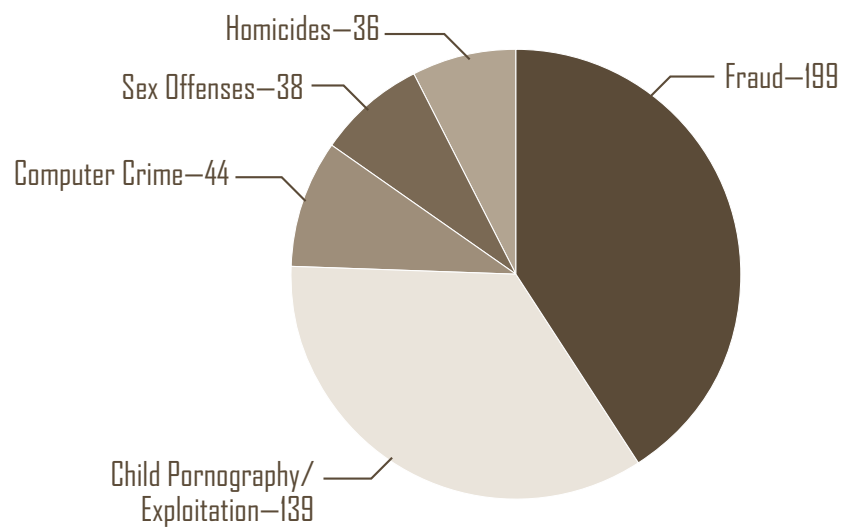
STATISTICS FOR FY 2003

The following tables and charts depict the San Diego RCFL's accomplishments during FY 2003.

<i>Casework</i>	
Number of service requests	707
Participation in search and seizure operations	117
Number of examinations performed	590

Submissions by Crime Type

During FY 2003, the San Diego RCFL received the most submissions for assistance with fraud cases.



Training

Law enforcement officers trained in search and seizure techniques, computer investigation techniques, and/or computer forensics	698
Number of detailees who received FBI sponsored training	16

Personnel

New detailees	1
Number of detailees returned to home agencies	3
Total number of detailees	16



NORTH TEXAS RCFL

Year Established
2000

Director
Michael S. Morris

Service Area
137 counties, serving a population of over seven million, and a law enforcement community composed of 30,000 law enforcement officers.

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

"Our dedication to cutting-edge technology has made us one of the most prestigious computer forensics laboratories in the RCFL community. I am very proud of the vision of our member agencies and especially proud of the people that make the magic happen every day. Each day begins and ends with challenges. The dedication and integrity of our forensic Examiners are envied by many and rivaled by few."

- Michael S. Morris, Director
North Texas RCFL

INTRODUCTION

In the late 1990s, there were only eight computer Forensic Examiners in North Texas (two from local police departments and six from Federal agencies) serving a population of over seven million people. Clearly, the odds were not on the side of criminal justice. Just as in San Diego, there was too much work and not enough skilled computer Forensic Examiners on hand. If San Diego was blazing a new path, North Texas was ready to follow in their wake.

In 2000, the FBI formed a coalition of area law enforcement agencies with the sole purpose of establishing an RCFL in the North Texas region. Their vision became reality when the North Texas RCFL opened for business with eleven Examiners detailed from eight participating agencies. On that day, the odds tipped back in favor of law enforcement.

Like their predecessors in San Diego, the North Texas RCFL was a welcomed resource that quickly became a genuine success. In their short, but illustrious history, the North Texas RCFL has supported a number of national investigations including Enron and the events surrounding 9/11.

Because of the added resources provided by the North Texas RCFL, the law enforcement community is now having their computer forensics needs met in a timely manner.

PROGRESS & ACCOMPLISHMENTS

In FY 2003, after being in operation for almost two years, the RCFL moved from its 5,500 square foot facility to a spacious, modern 15,000 square foot facility. Construction began in January 2003 and was completed in May of the same year. In June, the North Texas RCFL made a seamless transition to its new quarters, which has two conference rooms, two evidence review rooms, and a 1,200 square foot training room containing state-of-the-art computer and training equipment. The training facility can accommodate up to twenty-three Examiners. In FY 2003, the North Texas RCFL put the training room to good use in presenting "Image Scan" and a host of other training tools to 682 officers, effectively teaching them how to successfully recognize, seize and preserve digital evidence.

Many computer forensic laboratories measure their progress by the amount of data they process. During FY 2003, the North Texas RCFL examined 850 computers, 3,800 3.5 inch diskettes, 2,900 CDs, 500 loose hard drives and 280 various media cards, totaling 26.4 terabytes of data. If printed, this many terabytes is equal to 13,177,990,500 typed pages. That's enough paper to circle the earth approximately 92 times.

"In FY 2003, the North Texas RCFL trained 682 officers on computer related issues and how to recognize, seize and preserve digital evidence."

In FY 2003, the North Texas RCFL processed 26.4 terabytes of data.

CHALLENGES AHEAD

The North Texas RCFL set its sights on achieving a number of challenging goals during FY 2004. The first is to obtain ASCLD/LAB accreditation. Director Morris believes that accreditation will strengthen the RCFL's service offerings, and will set a positive example for other digital evidence laboratories operating in the state and the rest of the Nation.

Other goals for FY 2004 are to:

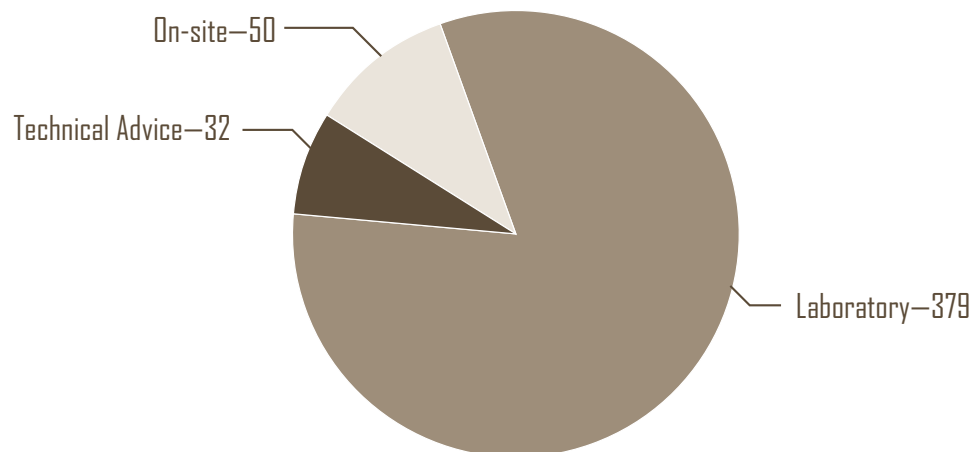
- Enhance lab capabilities to handle a projected increased caseload
- Recruit and train six additional Examiners
- Continue education and training for current Examiners
- Enhance the no-cost training program for area law enforcement on digital evidence and computer related issues
- Raise law enforcement's awareness that computers and other digital devices contain valuable evidence, no matter what the nature of the crime
- Collaborate with state and Federal prosecutors to create search warrant language and consent-to-search forms pertaining to computers and digital evidence
- Continue evaluating the services provided to agencies in its service area
- Continue working on research and development projects

STATISTICS FOR FY 2003

The following tables and charts depict the North Texas RCFL's accomplishments during FY 2003.

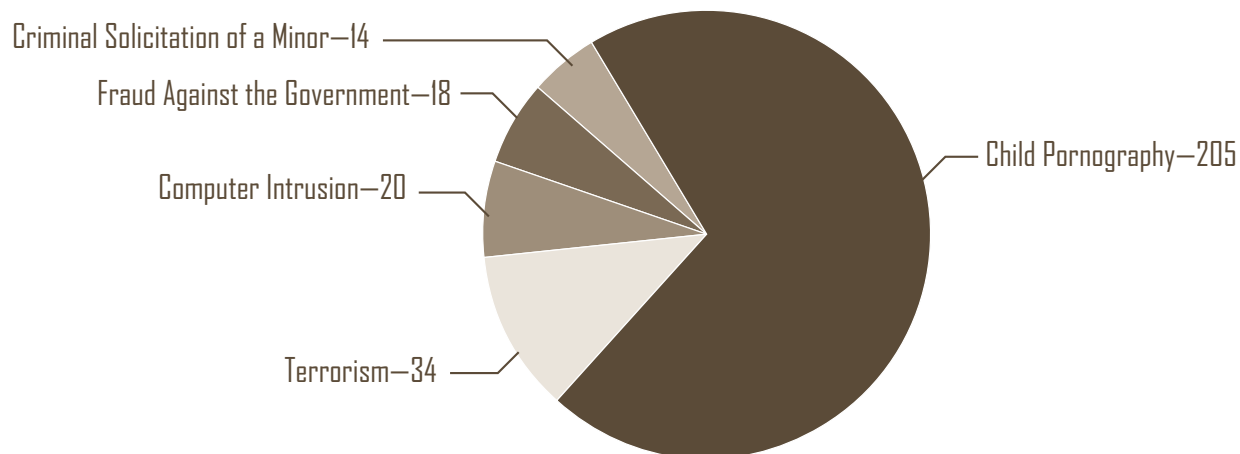
<i>Casework</i>	
Number of service requests	461
Participation in search and seizure operations	50
Number of examinations performed	379

Types of Assistance



Submissions by Crime Type

During FY 2003, the North Texas RCFL received the most submissions for assistance with child pornography/exploitation cases.



Training

Law enforcement officers trained in search and seizure techniques, computer investigation techniques, and/or computer forensics	682
---	-----

Number of detailees who received FBI sponsored training	15
---	----

Personnel

Number of detailees	15
---------------------	----

Number of detailees returned to home agencies	3
---	---

Total number of detailees	15
---------------------------	----



CHICAGO 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
- Illinois Attorney General's Office
- Illinois State Police
- Palatine Police Department
- University of Illinois Police Department
- Will County Sheriff's Department

"The Participating Agencies and our Examiners have worked long and hard to build this laboratory. Their dedication and diligence has made the Chicago RCFL an invaluable asset to the Chicagoland law enforcement community, while positioning us to serve our Nation as a leader in the processing of digital evidence."

—Rick Voss, Director
Chicago RCFL

INTRODUCTION

With a rich and vibrant history, Chicago is one of our Nation's greatest cities. However, as with any big city, Chicago has its share of crime, with many of these illegal acts involving computers and assorted types of electronic equipment. According to FBI Special Agent in Charge Thomas Kneir, "We see it almost in every case now; it's just the way business is done."

With a highly motivated law enforcement community behind them, Chicago showed why they sorely needed additional computer forensics expertise, and how their existing resources could successfully support an RCFL in their region. FBI Director Mueller agreed, and announced in 2002 that Chicago would join the RCFL network the following year. The Chicago RCFL opened its doors just five months after the announcement, on March 3, 2003, in the Old Customs House in the downtown area.

"The crooks nowadays know how to use a computer and are not afraid of it."

—Chief David Peters,
University of Illinois,
Chicago Police

PROGRESS & ACCOMPLISHMENTS

The Chicago RCFL began operating with ten Examiners, one administrative assistant, and five information technology support staff from eight Participating Agencies. The staff working in the Chicago RCFL didn't have much time to become accustomed to their new, state-of-the-art, 17,000 square foot facility. They had too much work to do, as is evident by the following major milestones achieved during FY 2003:

- Processed 20 terabytes of data
- Installed 18 Examiner workstations and an Imaging Room
- Outfitted an Evidence Control Room
- Secured Internet access and a T-1 connection
- Tested and helped develop a bar code based evidence control system
- Implemented a case management system
- Outfitted a twenty-seat classroom
- Developed two training courses
- Established standard operating procedures
- Instituted a quality assurance program
- Implemented a Chicago RCFL Web site

During FY 2003, the Chicago RCFL increased the number of Participating Agencies by one, adding the Will County Sheriff's Department to its ranks.

*In seven months,
the Chicago RCFL
processed 20
terabytes of data.*

Training—One of the Chicago RCFL's goals is to train and educate Federal, state and local law enforcement personnel and prosecutors regarding the forensic examination of digital evidence as it relates to the investigation and prosecution of computer-related or technologically facilitated crime. During FY 2003, the Chicago RCFL trained 145 law enforcement officers.

To this end, the RCFL, together with CART, has delivered several no-cost, Examiner-taught classes, including:

Collection, Handling and Use of Digital Evidence—This "Bag and Tag" class was designed for front line investigators interested in obtaining training on the seizure and handling of computer-related evidence.

Image Scan—This Linux based utility course was developed by Rod Gregg, an Examiner with the North Texas RCFL, and is used by Crimes Against Children investigators during field investigations.

CHALLENGES AHEAD

The main challenge facing the Chicago RCFL as it heads into the first full fiscal year of operations is to reduce the backlog for requests for service. Therefore, the Chicago RCFL developed a twofold plan of action aimed at greatly reducing or completely eliminating the backlog in the foreseeable future:

Increase Staff Levels—To better manage the number of service requests and the amount of data needing processing, the Chicago RCFL plans to expand its workforce to twenty-one. Any additional Examiners will be drawn from Participating Agencies already entered in the RCFL Program, which will detail personnel to the laboratory.

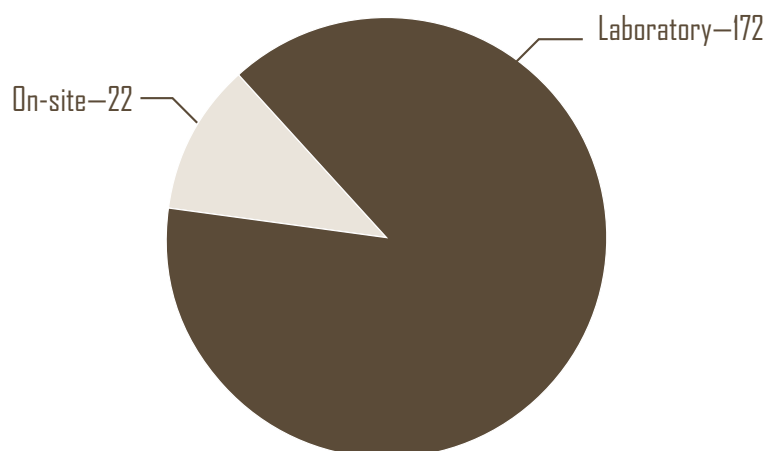
Improve the Infrastructure—To reduce the turnaround time for service requests, the Chicago RCFL is installing a fibre channel local area network and a 15 terabyte storage area network. These additional resources will significantly strengthen the Chicago RCFL's ability to process digital evidence, enabling the Examiners to provide their findings to the investigators and prosecutors in a more timely and expeditious manner.

STATISTICS FOR FY 2003

The following tables and charts depict the Chicago RCFL's accomplishments during FY 2003.

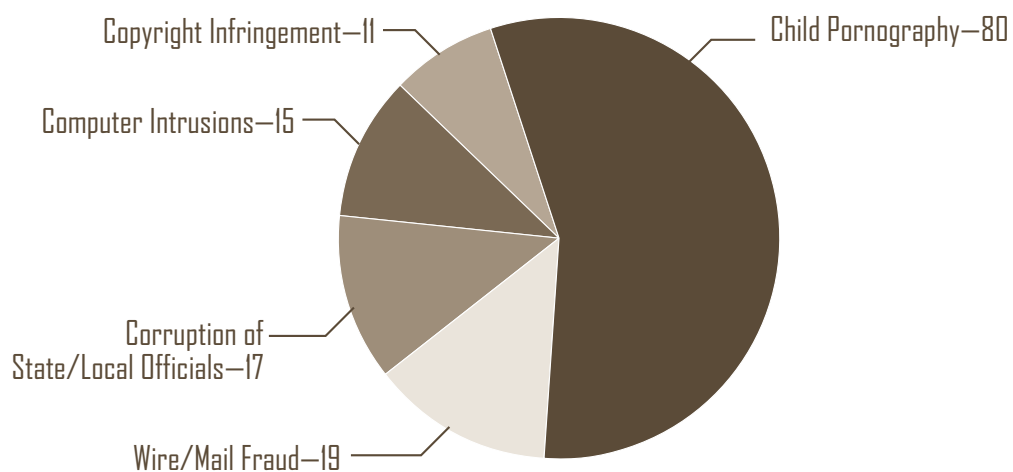
<i>Casework</i>	
Number of service requests	222
Participation in search and seizure operations	22

Types of Assistance



Submissions by Crime Type

During FY 2003, the Chicago RCFL received the most submissions for assistance with child pornography cases.



Training

Law enforcement officers trained in search and seizure techniques, computer investigation techniques, and/or computer forensics	145
Number of detailees who received FBI sponsored training	16

Personnel

Total number of detailees	16
---------------------------	----



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
- Overland Park, Kansas Police Department
- U.S. Attorney's Office—District of Kansas
- U.S. Attorney's Office—Western District of Missouri

"Teamwork is key... That's why RCFLs are so significant. It's not just the sharing of supplies and it is not just sharing equipment. It's the sharing of personnel, training, experience, and specialization."

—Thomas J. Maiorana, Director
Heart of America RCFL

INTRODUCTION

The Participating Agencies that compose the Heart of America RCFL (HARCFL) exemplify the level of commitment and partnership that establishing an RCFL requires.

Although the desire to have an RCFL was clearly evident, the coalition of law enforcement agencies from Missouri and Kansas first had to demonstrate on paper and through meetings with FBI personnel just how they would meet the NPO's criteria of having:

- Strong community-wide support for an RCFL
- A commitment to securing a qualified Director and staff
- A large pool of available and qualified talent
- An accessible location

The coalition was successful in their quest to bring an RCFL to Kansas City. In 2002, FBI Director Mueller selected the region to receive an RCFL the following year.

PROGRESS & ACCOMPLISHMENTS

The major accomplishment of FY 2003 for the HARCFL was opening for business. On December 18, 2002, the coalition held their first Local Executive Board meeting and selected Thomas J. Maiorana to serve as the first RCFL Director. On May 19, 2003, construction of the HARCFL was completed, and on the same day, furniture and equipment were moved into the new space.

The HARCFL officially opened on July 9, 2003, with such luminaries in attendance as Todd

Graves, U.S. Attorney for Missouri, and Kansas Attorney General Phil Kline, who said, "Justice is a goal that will be achieved, thanks to your leadership and collaboration." The event was widely covered by the major television network affiliates, and articles about the HARCFL appeared in the *Kansas City Star* and the *Sun-News of the Northland*.

Although the HARCFL was open for just three months during FY 2003, it successfully processed 1.9 terabytes of data.

CHALLENGES AHEAD

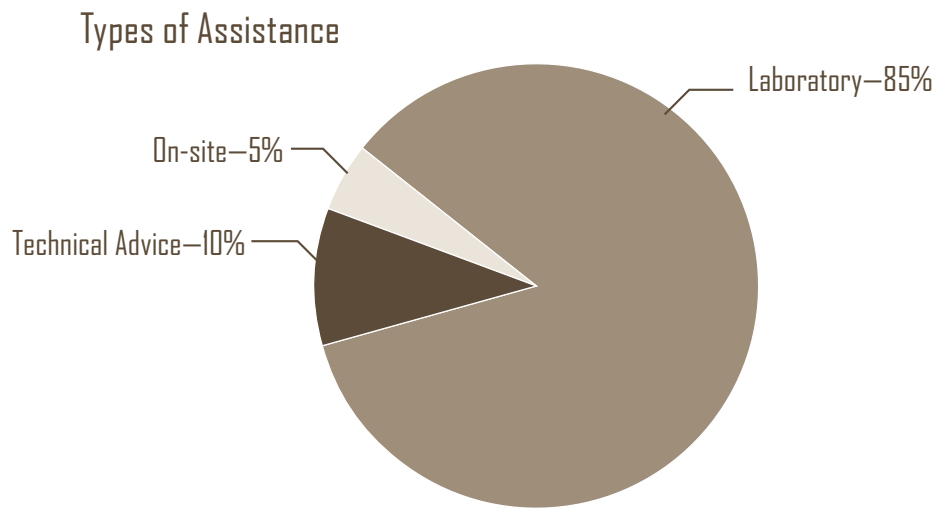
In FY 2004, the HARCFL will have celebrated its first full year of operations. Although getting a new organization off the ground is always a challenge, the HARCFL is doing well in all respects, and has set the following goals for the year:

- Continue education and training for the current Examiners
- Enhance the lab's capabilities and services
- Raise awareness regarding the services offered by the lab among the approximately 800 law enforcement agencies in the HARCFL's service area
- Provide training to law enforcement agencies regarding digital evidence

STATISTICS FOR FY 2003

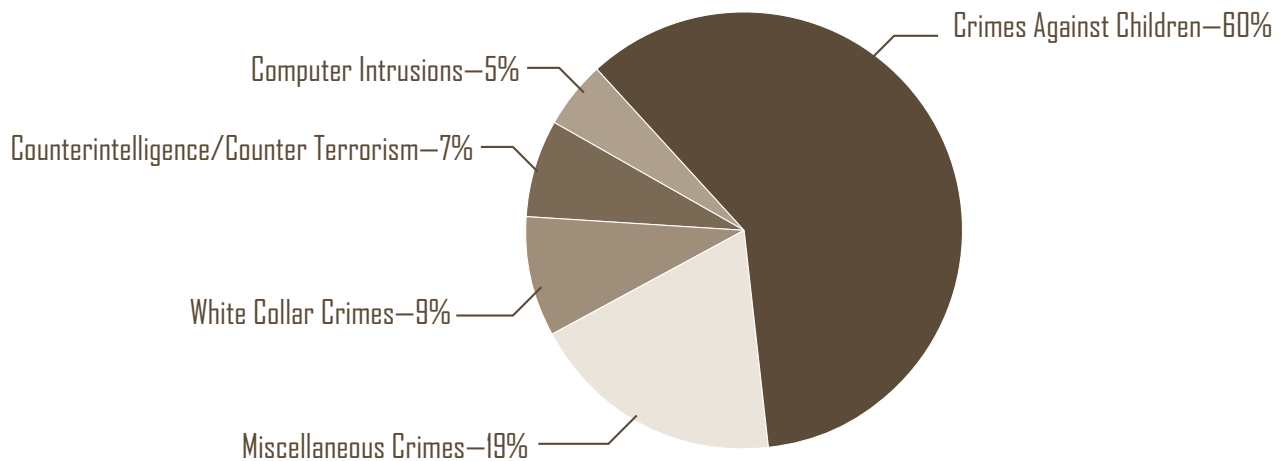
The following tables and graphs display the HARCFL's accomplishments during FY 2003. It should be noted that the facility was only open for the last quarter of FY 2003.

<i>Casework</i>	
Number of service requests	76
Participation in search and seizure operations	7
Number of examinations performed	18



Submissions by Crime Type

During FY 2003, the Heart of America RCFL received the most submissions for assistance with crimes against children/child pornography cases.



Training

Law enforcement officers trained in search and seizure techniques, computer investigation techniques, and/or computer forensics	16
---	----

Number of detailees who received FBI sponsored training	9
---	---

Personnel

Total number of detailees	9
---------------------------	---



ACKNOWLEDGEMENTS

The RCFL National Program Office would like to thank the RCFL Directors, the Local Executive Board members, and the many Participating Agencies and detailees whose tireless efforts, dedication and commitment to excellence and innovation have made us the premier computer forensic laboratory network in the country. Without the following Participating Agencies, the RCFL Program would not be possible:

California Highway Patrol

Chicago Police Department

Chula Vista Police Department

Cook County Sheriff's Office

Dallas Police Department

DHS—Immigration and Customs Enforcement

Drug Enforcement Agency

Escondido Police Department

Federal Bureau of Investigation

Garland Police Department

Grand Prairie Police Department

Illinois Attorney General's Office

Illinois State Police

Johnson County, Kansas Sheriff's Office

Kansas Bureau of Investigation

Kansas City, Kansas Police Department

Kansas City, Missouri Police Department

La Mesa Police Department

Lawrence, Kansas Police Department

Lenexa, Kansas Police Department

Missouri Highway Patrol

Naval Criminal Investigative Service

Northern District of Texas, United States Attorneys Office

Overland Park, Kansas Police Department

Palatine Police Department

Plano Police Department

Richardson Police Department

San Diego District Attorney's Office

San Diego Police Department

San Diego Sheriff's Department

Texas Internet Bureau

University of Illinois Police Department

U.S. Attorney's Office

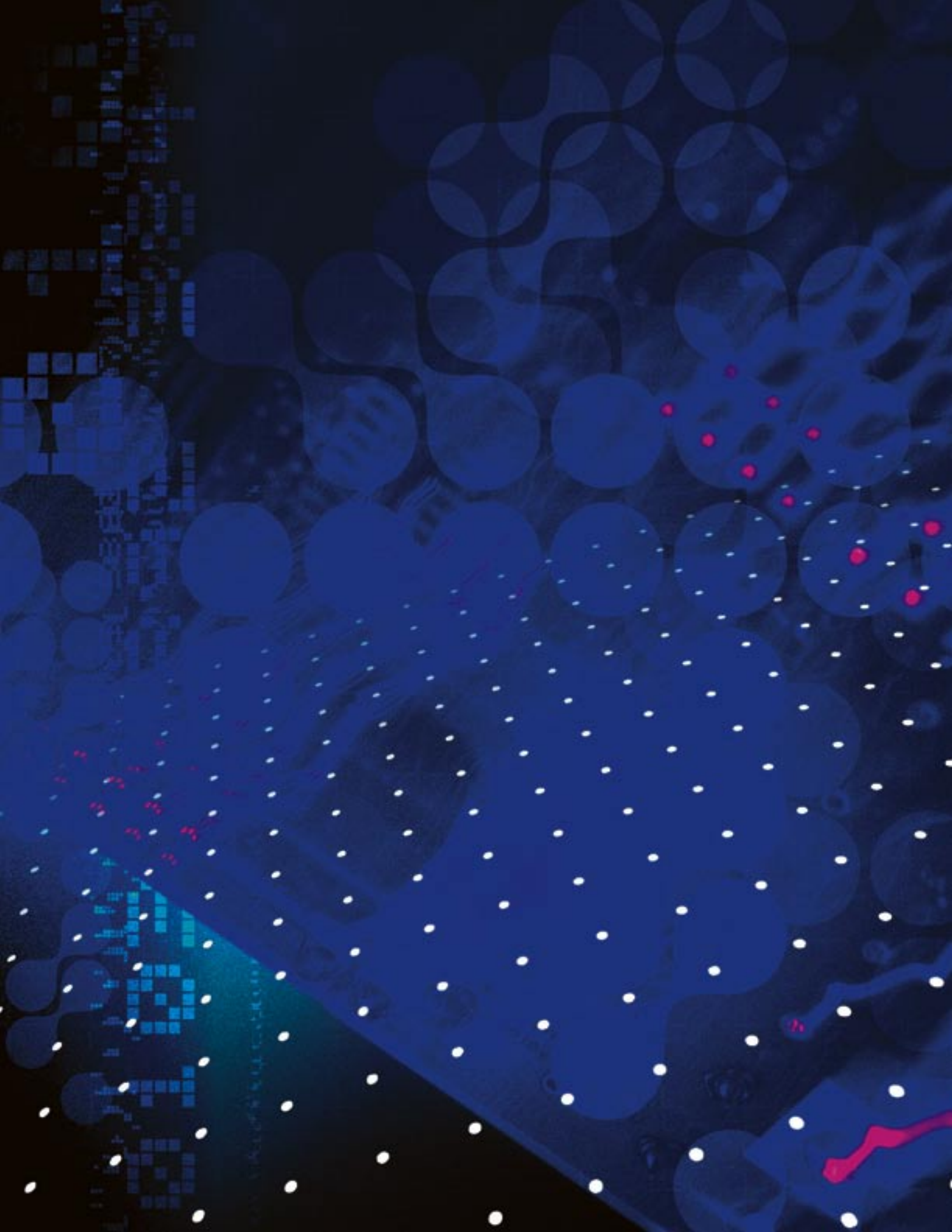
- District of Kansas
- Northern District of Texas
- Southern District of California
- Western District of Missouri

U.S. Border Patrol

Will County Sheriff's Department

A special thanks to FBI Director Robert S. Mueller III and Assistant Director Kerry E. Haynes, Investigative Technology Division, for their continued support of the RCFL Program.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



ENGINEERING RESEARCH
FACILITY
BLDG. 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

"The RCFL Program—America's
Premier Computer Forensics Network"



REGIONAL COMPUTER
FORENSIC LABORATORY