Digital Investigation (2004) 1, 177–182

Digital Investigation

www.elsevier.com/locate/diin

Building FBI computer forensics capacity: one lab at a time

Douglas A. Schmitknecht

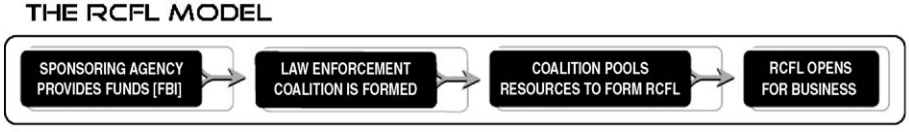
FBI, USA

The Federal Bureau of Investigation (FBI) is on a mission: to strengthen law enforcement's computer forensic capabilities throughout the United States. How are we fulfilling such a sweeping and ambitious mandate? Through an innovative initiative entitled the Regional Computer Forensic Laboratory (RCFL) Program. RCFLs provide much needed computer forensic expertise and training to thousands of law enforcement personnel. Although the demand remains high for skilled computer forensic Examiners — a common challenge facing law enforcement worldwide — RCFLs are doing their part to level the playing field. If properly administered, the FBI believes that the RCFL model can be duplicated from Prague to Portland, with the same level of success.

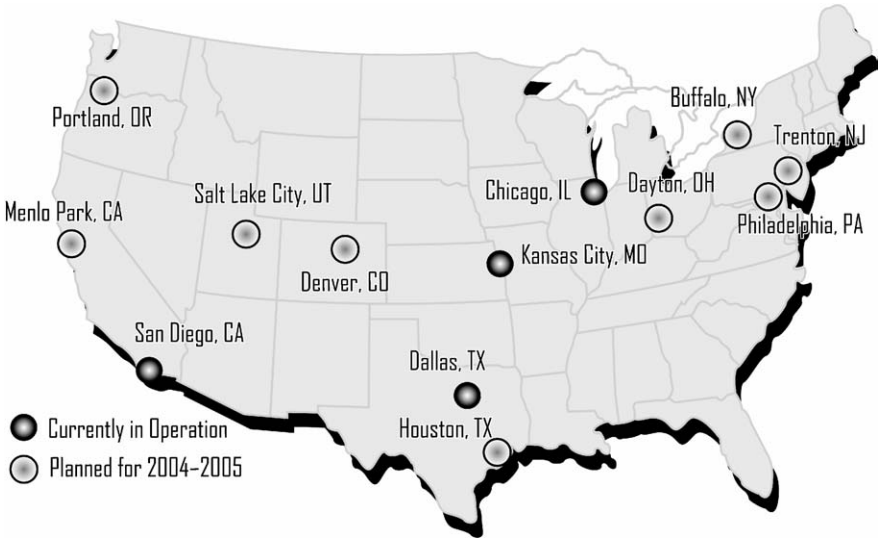
The RCFL "model"

The RCFL model is based on two guiding principles: cooperation and partnership. Although the Program is technical in nature, collaboration between an array of law enforcement agencies is the main driver behind the Program's continued success. FBI Director Robert S. Mueller III calls the RCFLs, "...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."

The actual RCFL "model" is based on the formula developed by the San Diego RCFL. The San Diego RCFL began as a test project in 1999, where a coalition of law enforcement agencies in Southern California pooled their personnel and funding resources to create an FBI-sponsored, single-service computer forensics laboratory. The San Diego agencies looked to the FBI for training and technical support, and in response, the FBI's Computer Analysis Response Team (CART) program was selected to provide training and certification to the RCFL Examiners. Moreover, the FBI assumed a majority of the start-up costs, while the other coalition members donated personnel to staff the new lab. Within a matter of months of becoming operational, the San Diego RCFL established a clear standard for the effective and efficient examination of digital evidence, enabling them to



1742-2876/$ - see front matter
doi:10.1016/j.diin.2004.07.007



address the computer forensic needs of area law enforcement.

With only eight Examiners serving a population of over seven million people, the FBI's Dallas Field Office and their local counterparts were working under similar circumstances as their San Diego colleagues — too much casework and not enough skilled computer forensic Examiners on hand. The FBI's Dallas Field Office followed San Diego's model and spearheaded a coalition of area law enforcement agencies with the goal of establishing an RCFL in the North Texas region. In 2000, their vision became reality when the North Texas RCFL opened for business with eleven Examiners detailed[1] from eight participating agencies. Like their predecessors in San Diego, the North Texas RCFL was a welcomed resource that quickly became a genuine success.

A program emerges

With the passage of the US Patriot Act in 2001, and an impressive and growing list of accomplishments, the US Congress directed the FBI to launch more RCFLs across the country. Therefore, in addition to the facilities in San Diego and North Texas, RCFLs were established in Chicago, Illinois and Kansas City, Missouri in 2003. Nine more laboratories will join the Program over the 2004—2005 time period, bringing the total number of RCFLs to 13.

[1] Participating Agencies "detail" employees to serve in an RCFL usually for two or three year terms. These individuals remain as employees of their home agencies, and return there upon concluding their assignment.

Existing and future RCFL sites

As with any new program, it is essential to have a series of institutionalized procedures and processes in place to manage both the day-to-day operations and to guide future growth. In 2002, the FBI established the RCFL National Program Office (NPO) to assume this role and to facilitate the creation of new RCFLs. Additionally, the NPO supports the laboratories by:

- Providing technical assistance to ensure consistent quality management of each laboratory.
- Institutionalizing the policies, practices, and legal processes regarding the establishment and governance of RCFLs.
- Cultivating working relationships between law enforcement, the private sector, academia and other government agencies by serving as a national clearinghouse for the exchange and dissemination of information among these entities.
- Serving as an advocate for the Program before key constituent groups.
- Developing new digital evidence forensic tools.
- Developing training curricula for digital evidence Examiners and law enforcement officers.
- Coordinating and communicating training initiatives and tool development efforts for use by the law enforcement community.

The NPO is physically located at the FBI's offices in Quantico, Virginia. Since the RCFLs are spread across diverse, geographical locations, one of the NPO's top priorities is to maintain communications with the field. The NPO holds conference calls with RCFL directors, organizes bi-annual meetings and

holds an annual RCFL conference, which is open to any law enforcement officer.

Standardization

To ensure uniformity throughout the Program, all FBI-sponsored RCFLs must follow a well-defined Quality Assurance Program, complete with FBI-approved Standard Operating Procedures and Quality Assurance Manuals. These standards govern policies and procedures concerning evidence handling; search and seizure operations; the examination of seized electronic equipment, including computers; and courtroom testimony. The notion of following a uniform set of procedures also applies to data gathering. Throughout the fiscal year (FY), the RCFLs enter case information into a centralized database managed by headquarters. This information is used in part to create the Program's annual report, to track the Program's progress, to identify where resources are needed, and to measure the Program's performance for the year.

Each RCFL facility prepares to seek accreditation from the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB). The benefits of accreditation, including:

- *Improves quality* — Accreditation will heighten the quality of the RCFLs services because an independent, impartial and objective team of experts will review the laboratory's findings and operations.
- *Strengthens operations* — Accreditation ensures that an RCFL is abiding by criteria that are designed to assess performance, while also strengthening operations.
- *Establishes standards* — With accreditation, the general public and the users of the RCFL are assured that the laboratory is following established and widely accepted standards.
- *Enhances quality control* — Accredited laboratories must follow appropriate quality controls and quality assurance procedures.
- *Guarantees Examiner qualifications* — ASCLD/LAB requires that laboratories have certified Examiners on staff. All RCFL Examiners must undergo the FBI's CART certification process, and may not perform examinations independently until doing so. (Trainees may need anywhere from six months to a year of training before they are certified.) Certification implies that an individual has a certain body of knowledge, and counters a recent trend where an investigator is deemed an "expert" after taking a short course in computer forensics.
- *Protects evidence* — ASCLD/LAB accreditation focuses on evidence handling procedures, to ensure that evidence is not damaged or misplaced.
- *Ensures accurate results* — Accreditation can enhance forensic results by requiring sufficient written protocols that serve as an empirical basis for the most basic and complex procedures.

The North Texas RCFL recently requested an ASCLD/LAB inspection and expects to become the first RCFL to obtain this prestigious accreditation. All RCFLs are expected to follow this lead.

A powerful network

As new RCFLs are formed, they gain access to a powerful, and growing network of resources and manpower. For instance, if a case is particularly complex, or if a specific expertise is needed, an RCFL Director can ask the NPO to identify what resources are available to them within the Program. The fact that all RCFL Examiners are CART certified and proficient in the Program's operating procedures qualifies them to step into national service at a moment's notice. The Pentagon bombing investigation illustrates this point, and most recently, an Examiner assigned to the Chicago RCFL provided expert computer forensics support for an investigation involving a suspected terrorist. While examining the five computers associated with the case, he used Netcase as one of the primary forensic tools. Although all the text was in a foreign language (Arabic), he successfully identified several documents that pertained to terrorist activities. The suspected terrorist was indicted by a federal grand jury this past June for providing material support to al Qaeda, and for obtaining and using fraudulent travel documents.

Finally, all RCFL Examiners must obtain a Top Secret clearance, which the NPO facilitates upon their hiring. This allows the immediate sharing of personnel without constraints and enables RCFL Examiners to assist with any Federal, state, or local investigation. In today's post-*9/11* environment, having this capability is especially critical.

RCFLs in action

Any law enforcement agency within the RCFL's service area may request digital evidence technical support, on-site collection assistance, or training.

Every FBI-sponsored RCFL offers the following range of services.

Computer forensics expertise

Computer forensics expertise may fall into the following categories:

- Pre-seizure consultation
- On-site seizure collection
- Duplication, storage and preservation of digital evidence
- Impartial examinations of digital evidence
- Documenting the work and nature of requests in preparation for testimony
- Courtroom testimony

In FY 2003, the RCFL Program accepted 1444 requests for service, participated in 196 search and seizure operations, and conducted 987 computer forensic examinations. To request an RCFL's assistance, a law enforcement agency must complete and submit a simple form to the RCFL. This process is extremely convenient, as each RCFL has a dedicated website with a specific section devoted to requesting assistance.

RCFLs support a variety of white collar, violent, and cyber crimes. These investigations include fraud, child pornography, terrorism, computer intrusions and Internet crimes just to name a few. Examples of some of the RCFL success stories follow.

Internet stalking case
In 1999, the state of California enacted one of the toughest cyber stalking laws in the US. Shortly after the law's passage, the San Diego RCFL supported an Internet stalking case that was brought to trial. An ex-husband impersonated his ex-wife over the Internet by engaging in ''cyber'' relationships with several men. He gave the men his ex-wife's phone number and urged them to call her. When authorities seized the suspect's computer and provided it to the San Diego RCFL for examination, at first, the Examiners found no direct evidence in the active files. In time, they unearthed over 500 ''chat'' logs in the unused portions of the hard drive detailing the ex-husband's illicit activities on the Internet. When this information was presented at trial in 2000, the suspect was convicted of felony stalking charges.

September 11 terrorist attack
Examiners from both the San Diego and North Texas RCFLs supported the ''PENTTBOM'' investigation, which was named after the terrorist attacks against the Pentagon, the World Trade Center, and the crash in Pennsylvania. The San Diego RCFL processed over 29 separate service requests, and examined over 40 computers and hundreds of pieces of loose media. Concurrently, the Lab provided technical and operational assistance to the FBI's Newark Division, which was inundated at that time. Meanwhile, the North Texas RCFL single-handedly processed over 50% of the digital evidence involving the aftermath of September 11. Thanks to the operational capabilities of all the RCFL Examiners, every request was processed in record time, providing key FBI personnel with results, at times, in a matter of hours.

Reclaimed data from melted computer terminal
A suspect rang the doorbell of his victim, fatally shot him five times in the face, and then set a computer in the victim's house on fire. The Dallas Police Department brought the once smoldering mound of plastic that was a computer, to the North Texas RCFL for examination. The Examiners replaced the computer's melted circuit board with the same exact model. As if that wasn't enough of a challenge, they next had to retrieve a floppy disk that was now shaped like an ''S.'' After removing the casing, putting it into a new sleeve, and repeatedly cleaning the disk, it finally yielded the valuable digital evidence that the Examiners so meticulously searched for. In this case, high technology took a back seat to perseverance, patience, and fierce determination.

Training

Training is the cornerstone of the RCFL Program, and as such, is one of the most sought after, highly regarded offerings of the Program. This training takes two forms:

1) *Training law enforcement personnel in a region* — Each RCFL is equipped with a modern computer classroom where they train law enforcement personnel regarding handling sensitive electronic equipment that becomes evidence, computer investigation techniques, and computer forensics. In FY 2003, the RCFL Program trained 1541 law enforcement officers in these techniques. The benefits of having a knowledgeable workforce in computer forensics are immeasurable. A highly trained work force will enhance the preservation of digital evidence, and will help prosecutors convict those individuals who use computer technology to facilitate a crime.

2) *Training RCFL detailees* — The NPO coordinates the training of all RCFL Examiners and Examiner candidates. These individuals receive six weeks of standard FBI-approved computer forensics training during their first year, and up to three weeks of training in computer techniques and tools thereafter. Many Examiners cite this training and certification as one of the major benefits of participating in the Program. In FY 2003, 56 RCFL Examiners received FBI-sponsored training, and six Examiners returned to their home agencies, further building computer forensics capacity in the San Diego and North Texas regions. Former Examiners can still access the FBI's prestigious training and certification resources thanks to the ''Associate Examiner Program.'' This program is critical in helping former Examiners hone their skills and to stay abreast of new technologies.

Image Scan

The FBI's CART program developed this Linux-based software tool to assist investigators with identifying potential evidence of crimes. This tool protects valuable computer evidence by booting up the computer using the Linux operating system. Image Scan mounts the hard drive in a read only manner, and then prompts the investigator to search for pictures files only. During this process, the tool logs every step taken by the investigator during this consent search process. Because Image Scan is primarily used during the investigative stage, it can determine if contraband is present on a seized computer. Currently, each RCFL assigns an Examiner to teach investigators how and when to apply this tool. To date, it has been used on hundreds of cases, and has helped bring child predators to justice.

Research and development

Each RCFL has a number of activities and services they perform, with research and development being one of them. Each RCFLs has its own unique needs, therefore, each laboratory is pursuing different technologies to meet specific requirements. Once a technology is sufficiently tested and approved, the application is recommended for use by all of the laboratories in the Program. Some of these technologies include the following:

Write blocker 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) — The North Texas RCFL developed the ''SAN'' or storage area network. A SAN is a single repository that contains data for an individual case, and enables the Examiner to load large amounts of data to a single location for examination and review by investigators. After being sufficiently tested in FY 2003, the SAN technology was exported to other RCFLs throughout the Program and the FBI.

The write blocker and SAN technologies both reflect the collaborative spirit of the RCFL Program. By taking the lead in developing new technologies, the Program is producing cutting-edge tools that benefit all of law enforcement.

Future plans

The NPO has identified two major goals aimed at strengthening the Program. They are:

- *Growing the program while maintaining quality* — Nine RCFLs are scheduled to join the Program over the 2004—2005 time frame. The NPO, in coordination with the representatives of each new RCFL, are establishing standardized procedures, quality controls, and processes for each facility.
- *Increasing agency participation* — In FY 2003, 38 law enforcement agencies participated in the RCFL Program. In order to keep pace with the casework, the RCFL Program has made a commitment to increase the number of participating Examiners and agencies involved with each facility. Increased involvement will continue to build capacity and capabilities for the regions served by each RCFL.

Conclusion

The Program's continued growth and long list of accomplishments are a testament to the original

RCFL model. This pilot project, which started in San Diego, has evolved into America's premier computer forensic laboratory network. As the great football coach Vince Lombardi once said, ''The achievements of an organization are the results of the combined effort of each individual.''

To request an RCFL information package, send an email to info@nationalrcfl.org, or visit our website on www.rcfl.gov.

Douglas A. Schmidtknecht is a nineteen-year veteran of the FBI. Prior to becoming the Chief of the RCFL National Program Office, he was a member of the FBI's elite Computer Analysis Response Team.