blogs.sans.org home about sans links

A team of GIAC Certified Forensic Analysts (GCFA) and their thoughts on Digital Forensic and Incident Response techniques and trends.

Interview: Darrin Jones, Director of New Mexico RCFL

Posted by jarocki on July 27, 2009 – 1:31 pm
Filed under Computer Forensics, Digital Forensic Law

The Regional Computer Forensics Laboratory (RCFL) Program is a partnership between the FBI and local, state, and federal law enforcement agencies. The Program provides forensics resources and advanced techniques that can be brought to bear on cases being worked by participating agencies. The first RCFL was established in 1999 in San Diego, California. This successful partnership between FBI and Southern California law enforcement led to fifteen more centers over the ten years that followed. One of the most recent is in Albuquerque, New Mexico.

Supervisory Special Agent Darrin Jones is the Laboratory Director of New Mexico RCFL and was key to it's establishment. I interviewed him recently to find out more about the Program.

Q: When and why did you get involved with the RCFL Program?

A: I've been in Albuquerque for about two years, prior to this assignment I worked at Quantico within the FBI's Operational Technology Division (OTD). The national RCFL program is managed from within OTD. So, I've been familiar with the program for many years and have always been incredibly impressed with how successful the RCFL program has been. I starting trying to get an RCFL in New Mexico almost immediately when I arrived. It's a long process, usually taking several years from start to finish.

Q: What does it take to start up a new RCFL?

A: As you would expect there are many requirements for starting an RCFL. The Director of the FBI makes the final selection from among submitted proposals. I will tell you though, I believe one of the most important factors is the demonstration of commitment from the proposed partnering agencies. In short, are the partnering agencies, in additional to the executive management of the local FBI office, willing to support the RCFL by detailing their personnel on a full-time basis and through management of the RCFL by participation on the local executive board.

Q: Do the RCFLs provide the same services, or do they have specialties?

A: All RCFLs are committed to providing examination of digital evidence at the highest possible standards. Each RCFL handles the types of digital evidence you would expect; computers, cellular telephones, etc. But, yes, some RCFL locations have developed centers of excellence for dealing with specific types of digital evidence. For example, if we encounter a particularly complicated case dealing with a niche technology we have the option to exploit the expertise located in another RCFL by requesting their assistance or simply transferring the evidence to that facility for processing.

Q: What sort of advanced techniques are used at the RCFLs?

A: We do employ sophisticated techniques at the RCFLs, in many cases we use tools that have been developed, tested and validated in-house for exclusive use by the FBI and within the RCFLs. However, I would suggest that what makes the RCFLs so successful is not super sophisticated technologies that may be used occasionally, instead it's the rigorous adherence to the every day processing of digital evidence. From the moment the an item of evidence enters an RCFL facility it is processed according to strict protocols and requires extremely thorough documentation. Another reason I think the RCFLs have done so well over the years is the training ALL examiners must complete before becoming a certified examiner. This training includes hundreds of hours in both commercial and internal FBI classes at locations all over the United States. A typical RCFL examiner can expect to spend a minimum of 18 months in this training process, and that's assuming some knowledge coming into the program.

Q: How can digital forensic analysts get involved with their nearest RCFL?

A: Generally speaking, the RCFLs don't "hire" anyone, there are exceptions but normally a person must be detailed to an RCFL by their participating parent law enforcement agency. In New Mexico's case examiners will be detailed from the FBI, the Albuquerque Police Department, the Bernalillo County Sheriff's Office, and the New Mexico State Police.

Q: I've heard there are internships, what are the requirements for participation?

A: Most RCFL internships are managed via FBI Headquarters, for example, FBI Honors Interns (see fbijobs.gov for internship details) are selected via the national process then detailed to a specific RCFL. However, RCFLs can create localized internship programs. One of the most exciting things about the New Mexico RCFL is the fact that we are

SEARCH

Find

SUBCRIBE TO OUR FEED

MOBILE DEVICE FORENSICS

FOLLOW US ON TWITTER

CATEGORIES

- Browser Forensics
- Certification and License
- Computer Forensic Hero
- Computer Forensics
- Computer Forensics and IR Summit
- Digital Forensic Law
- Drive Encryption
- eDiscovery

partnering with the University of New Mexico. There is only one other RCFL in the country to have such a relationship and we anticipate the NMRCFL will be able to offer several different internships to UNM students. We will be posting more details regarding these internships on the NMRCFL website, hopefully in the next several months.

Q: Are there any well known cases where the RCFL involvement was key?

A: Yes, there are several readily recognized cases that have hinged on digital evidence processed at RCFLs. The best thing to do is to take a look at the newsroom link on the national RCFL site, they post new cases there all the time.

References:

Introduction to RCFLs (Last Modified: 04/02/09), http://www.rcfl.gov/downloads/documents/intro_to_RCFLs.doc
National Program web site, http://www.rcfl.gov/
New Mexico RCFL web site, http://www.nmrcfl.org/

John Jarocki, GCFA Silver #2161, *is an Information Security Analyst specializing in intrusion detection, forensics, and malware analysis. He also holds GCIA, GCIH, GCFW and GSEC certifications and the Treasurer of NM InfraGard.*

Permalink | Comments RSS Feed - Post a comment | Trackback URL.

Post a Comment

Your email is *never* published nor shared. Required fields are marked *

Name *

Email *

Website

Comment

Post Comment

Email Investigations
Ethics
Evidence Acquisition
Evidence Analysis
Incident Response
Linux IR
Malware Analysis
Memory Analysis
Mobile Device Forensics
Network Forensics
Registry Analysis
Reporting
Reverse Engineering
Uncategorized
Windows IR
Write Blockers

COMPUTER FORENSICS TRAINING COURSES

SANS Computer Forensics Training

RECENT POSTS

Interview: Darrin Jones, Director of New Mexico RCFL
Security Intelligence: Introduction (pt 2)
Security Intelligence: Introduction (pt 1)
A big FAT lie
2009 Forensics Summit reviews

RECENT COMMENTS

Mike Worman on Perl Fu: Email Discovery
mikecloppert on Security Intelligence: Introduction (pt 1)
Robert Miller on A big FAT lie
trustedsignal on A big FAT lie
Lee Whitfield on A big FAT lie

ARCHIVES

Select Month

META

Log in

WordPress | Corporate Sandbox is designed by Rubiqube and is based on Sandbox. Supported by Blogsessive.