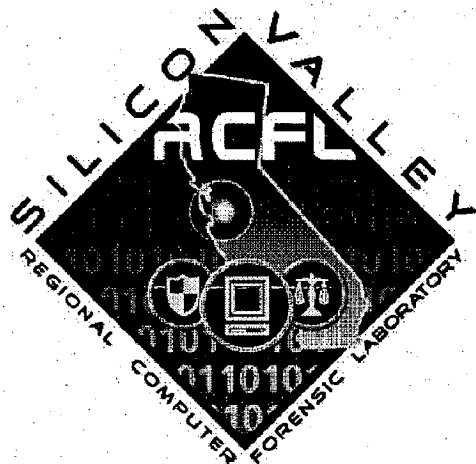




***Supporting Law
Enforcement's Needs in
the Digital Age***

4600 Bohannon Drive, Suite 200
Menlo Park, CA 94025
(650) 289-3000

www.rcfl.gov
www.svrcfl.net

info@svrcfl.net



Contact Information



b6
b7C

Silicon Valley Regional Computer Forensic Laboratory
Menlo Park, California
650.289-3000



b6
b7C



We Spend More of Our Lives using Digital Storage Devices

- Personal Computers (PC, Mac, Unix)
- Personal Digital Assistants (PDA's)
- Digital cameras & camcorders
- Digital Video Recorders
- Digital voice records
- Music players (iPod)
- Flash Memory Devices (thumb, CF, etc)
- Cellular telephones/digital pagers
- Optical Media (CD's, DVD's)

So, We Will Leave Many More Digital Trails!



No Secret

- Criminal activity using computers at all levels and across all criminal programs has been rising exponentially for the last 7 years
 - Terrorism
 - Counter Intelligence
 - Cyber (Hacking, Trade Secrets)
 - White Collar Crimes
 - Violent Crimes (incl. Sexual Predator)



As a Result:

- Traditional Crimes are producing enormous amounts of digital evidence
 - Cyber Crimes are producing complex digital evidence
 - Law enforcement, at all levels, is unprepared to process this data
-



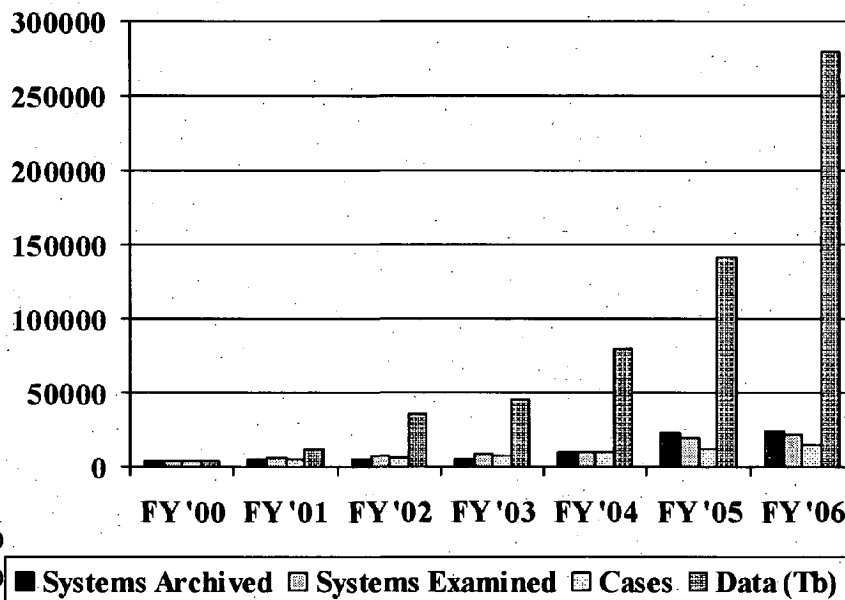
Why do we need RCFLs?

Case load:

- FY '00 - 3625
- FY '01 - 5195
- FY '02 - 6012
- FY '03 - 7323
- FY '04 - 9922
- FY '05 - 12167
- FY '06 - 14000

Data examined:

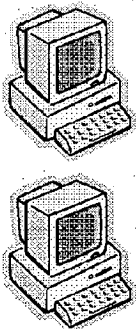
- FY '00 - 40 Tb
- FY '01 - 120 Tb
- FY '02 - 363 Tb
- FY '03 - 448 Tb
- FY '04 - 797 Tb
- FY '05 - 1420 Tb
- FY '06 - 2800 Tb



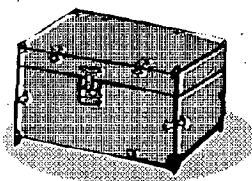


Examples

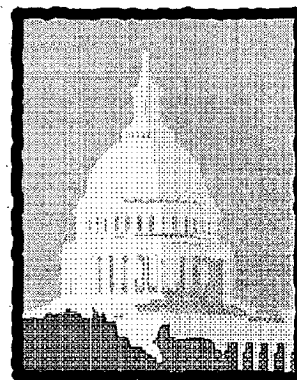
Data Processing



Tradebomb
1993



Okbomb
1995



Penttbom
2001 (7.4T)



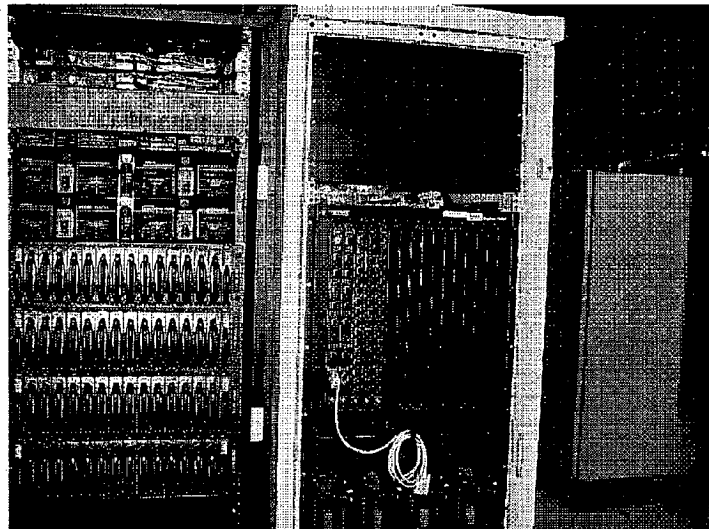
What to do with so much data?

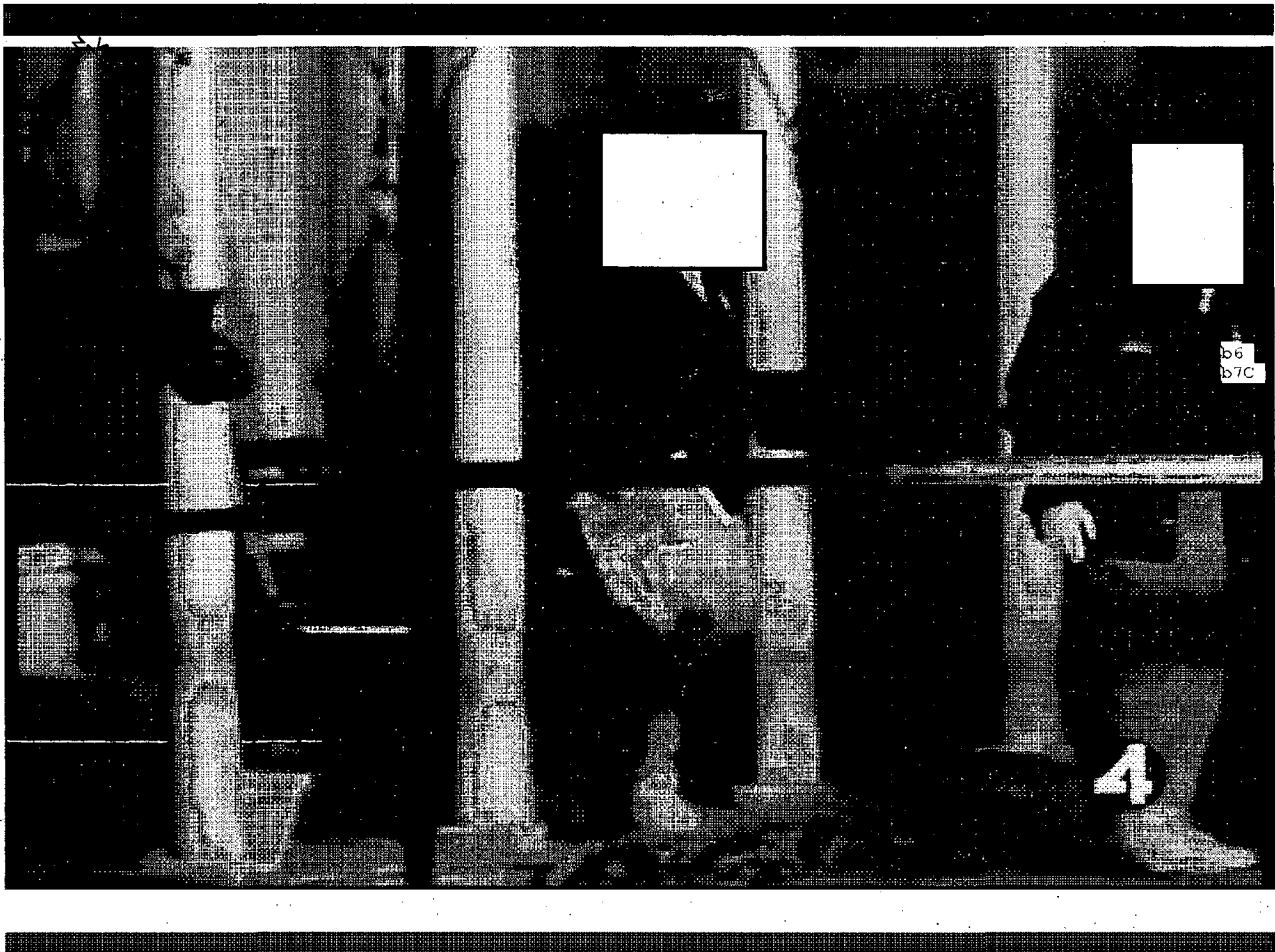
- In house processing?
 - Efficiency
 - Capability
 - County/State/Federal processing?
 - Turn around time
 - Private? (\$\$\$\$)
-



One Solution...

Regional
Computer
Forensic
Laboratory





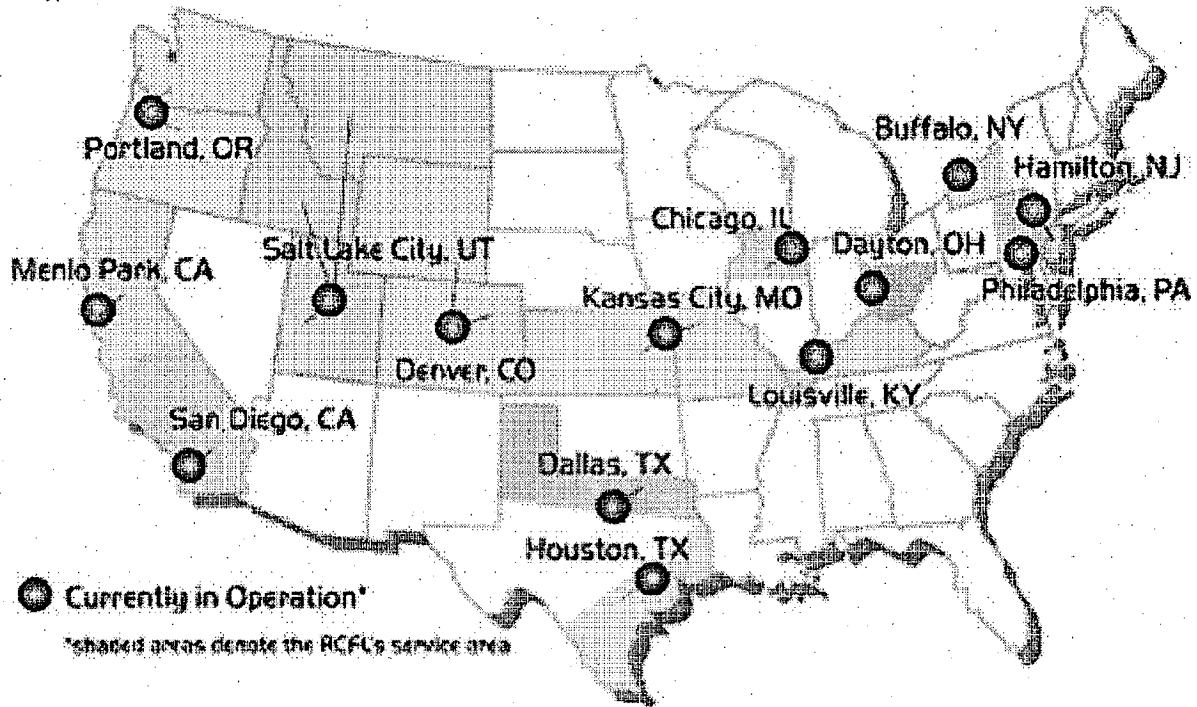


What is the RCFL Program

- A US based national network of 14 Digital Crime Laboratories serving approximately 1,000 law enforcement agencies
-



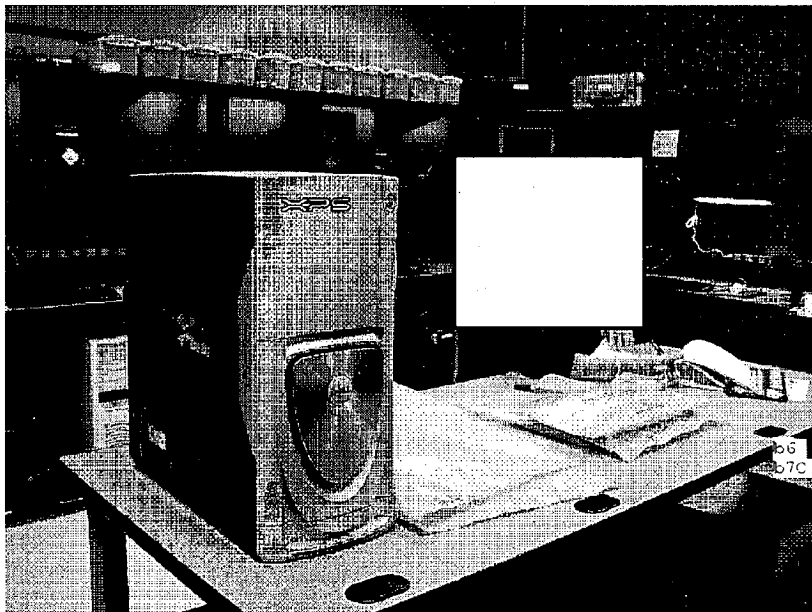
U.S. Digital Evidence Laboratories





What is an RCFL

- Single service forensic laboratory devoted entirely to the examination of computer/digital evidence in support of criminal investigations.





Regional Computer Forensic Laboratory

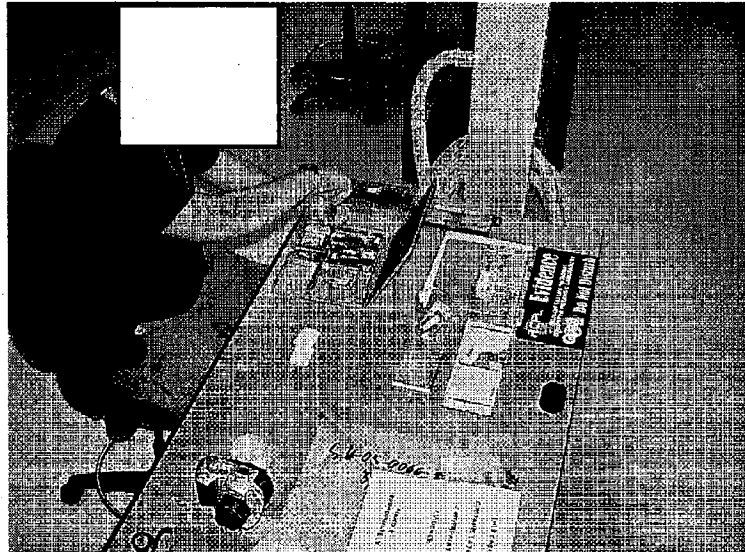
- The RCFL Program began in 1999 as a pilot project in San Diego, California in response to area law enforcement's growing demand for expert digital forensics services
 - The FBI's San Diego Field Office provided the funding and training to create a digital evidence laboratory; while local law enforcement agencies from all levels of government, donated personnel to staff the facility. This basic model is still followed today.
-



Regional Computer Forensic Laboratory

b6
b7c

- Because the San Diego RCFL was so successful in meeting law enforcement's digital forensics needs, a second RCFL was established in 2000 in Dallas, Texas





Regional Computer Forensic Laboratory

- Today there are 14 operational RCFLs serving law enforcement in 17 states. Each one is a full service digital evidence laboratory jointly staffed and operated by personnel from federal, state and local law enforcement agencies. There are approximately 100 participating agencies in the RCFL Program
-



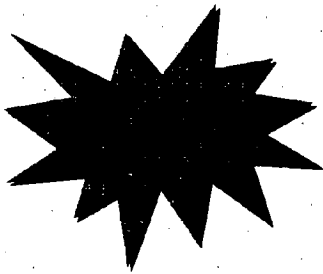
Regional Computer Forensic Laboratory

- Each RCFL provides high quality digital forensic services to law enforcement, and adheres to the FBI's laboratory quality standards to provide consistent, verifiable results.



ASCLD/LAB Accreditation

American Society of Crime Lab Directors/Lab Accreditation Board



- ✓ Provides an independent, impartial, and objective system for lab operational review
- ✓ Assesses lab quality assurance program including:
 - SOPs and Quality Manual
 - Proficiency testing
 - Continuing education
 - Other programs to help the laboratory give better overall service



RCFL Services

RCFLs provide the following services at no charge to their law enforcement customers—

- **Skilled scientific analysis** of digital evidence
 - **Complete and timely reporting** of examination results
 - **Expert courtroom testimony** within the region
 - **Regional technical resource** for support, advice, and training in matters of digital evidence, seizure, and examination
-



RCFL Services (cont'd)

FBI certified Examiners conduct examinations on a variety of electronic devices including:

- Hard drives
- Cell phones
- Audio/visual equipment
- Digital cameras
- PDAs
- Flash media
- Floppy disks/DVDs/CDs

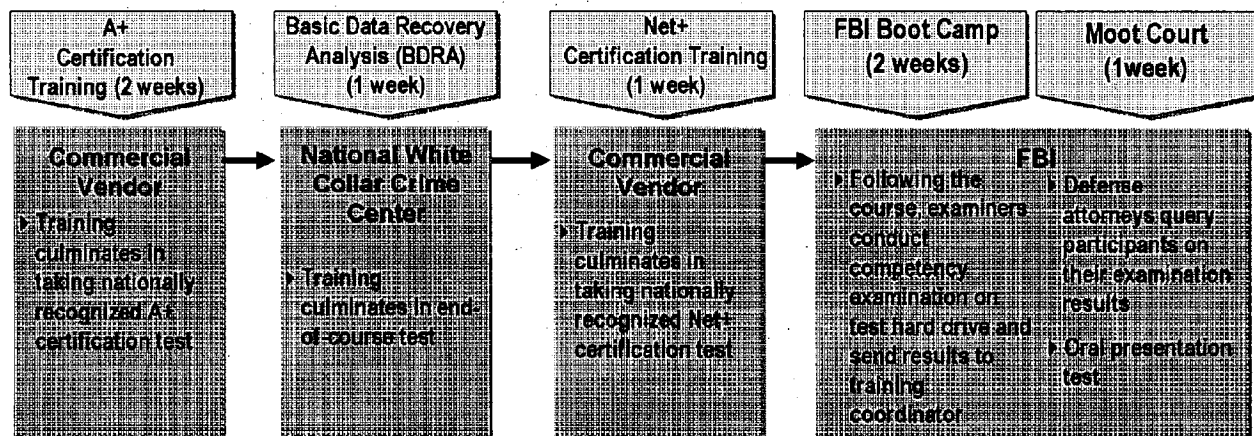


Case Prioritization (LEB/MOU)

- | |
|--|
| 1. Matters involving or affecting national security |
| 2. Imminent credible threat of serious bodily injury or death to persons known or unknown, including examinations of evidence necessary to further the investigation of an at-large or unknown suspect who poses an imminent threat of serious bodily injury to persons known or unknown |
| 3. Potential threat of serious bodily injury or death to person(s) |
| 4. Imminent credible risk of loss of or destruction of property of significant value |
| 5. Immediate pending court date, or non-extendable, outcome-determinative legal deadline |
| 6. Potential risk or loss of or destruction of property, or exam needed to further the investigation |
| 7. No credible or potential threat of bodily injury or death to person(s) and/or loss or destruction of property |



Examiner Training/Certification



Examiners must also conduct five searches and five exams under the supervision of an FBI-certified forensic examiner.

- Complete one advanced FBI-sponsored class per year
- Complete two additional outside classes per year
- Pass yearly proficiency test



Training

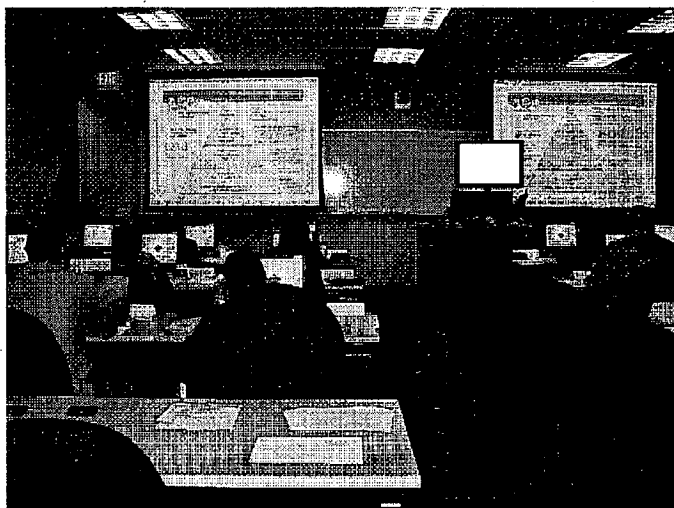
- Bag and Tag
- FTK Investigator
- Basic Data Recovery
- Image Scan

b6
b7c

www.svrcfl.org for training info

- Classroom available for other cyber/technical courses hosted by a participating agency

- LAW ENFORCEMENT ONLY





Funding

State and Local Provisions

Personnel

FBI Field Office Provisions

Personnel

SVRCFL Provisions '04-'06 \$3.9m (through Congressional Funding)

Facility Construction	\$929,000
Facility Infrastructure	\$700,000+
Facility Supplies/Furniture	\$140,000+
Facility Lease (annual)	\$537,000
Examiner ▪ Equipment (every 2-3 years) ▪ Training (every year) ▪ Workstations	\$42,000/examiner
Common Equipment (annual)	\$50,000
Media and Supplies (annual)	\$95,000
Training Room Equipment and Furniture	\$150,000



RCFL Casework - National

RCFLs follow uniform reporting requirements to evaluate the impact each laboratory is having on its own region and nationally. During FY05, the top 5 crime categories where RCFLs provided assistance were:

- Major Thefts/Violent Crime
 - Cybercrime
 - White Collar Crime
 - Organized Crime
 - Counterintelligence
-



It's about:

➤ "Sharing scarce knowledge and resources to deliver trusted results"



For further information:

[REDACTED]
Regional Computer Forensic Laboratory
Silicon Valley

4600 Bohannon Drive
Suite 200
Menlo Park, CA

b6
b7c

650.289-3000
[REDACTED]

www.rcfl.gov
www.svrcfl.net