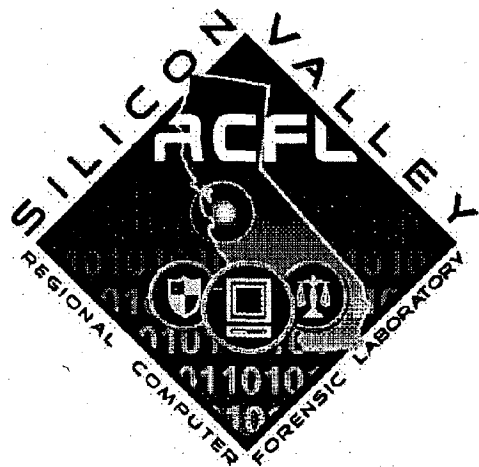




***Supporting Law
Enforcement's Needs in
the Digital Age***

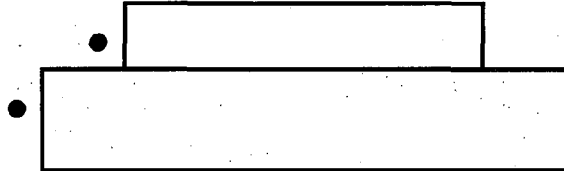
4600 Bohannon Drive, Suite 200
Menlo Park, CA 94025
(650) 289-3000

**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
 - @rcfl.gov

b6
b7C



Digital Storage Devices Surround us in our daily lives

- Personal Computers (PC, Mac, Unix)
- Personal Digital Assistants (PDA's)
- Cell Phones/Smart Phones (iPhone, etc)
- Digital cameras & camcorders
- Digital Video Recorders (Tivo)
- Digital voice records
- Music players (iPod)
- Flash Memory Devices (thumb, CF, etc)
- 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 10 years
 - Terrorism
 - Counter Intelligence
 - Cyber (Hacking, Trade Secrets, Child Pornography)
 - White Collar Crimes
 - Violent Crimes (incl. Sexual Predator)
-



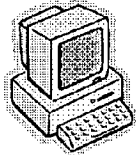
As a Result:

- 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
-

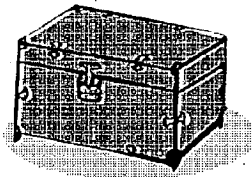


Examples

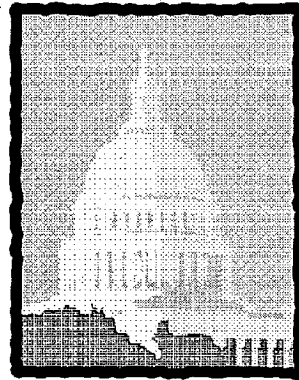
Data Glut



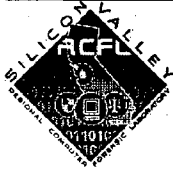
Tradebomb
1993



Okbomb
1995



Penttbom
2001 (7.4T)



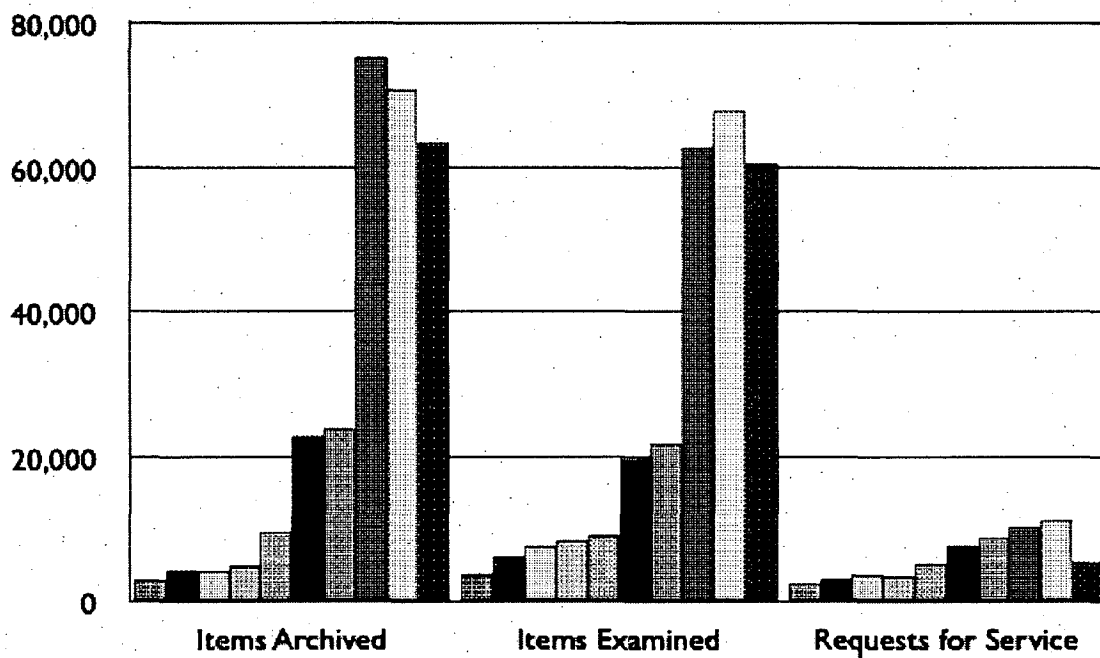
The Information Tsunami

- 1 byte: A single typed character
- 10 bytes: A single word
- 1 kilobyte: A very short story
- 1 megabyte: A small novel OR a 3.5-inch floppy disk (1.44mb)
- 100 megabytes: 1 meter of shelved books
- 1 gigabyte: A pickup truck filled with paper
- 100 gigabytes: A floor of academic journals
- 1 terabyte: 50,000 trees made into paper and printed with text
- 136 terabytes: The 17 million books in the Library of Congress if they were digitized



Why we need RCFL's

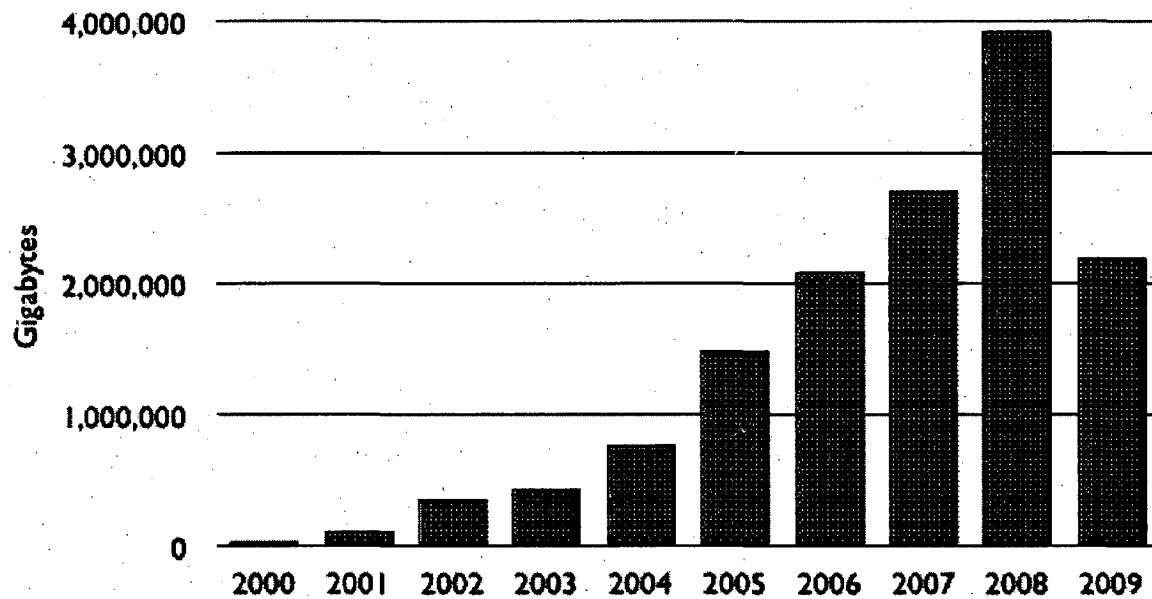
2000 to 2009 (4/1/09) -- All FBI and All RCFL's

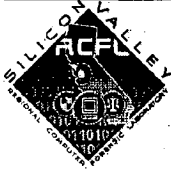




Why we need RCFL's

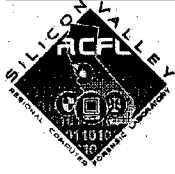
Data Archived and Examined 2000 to 2009 (4/1/09) - All FBI and RCFL's





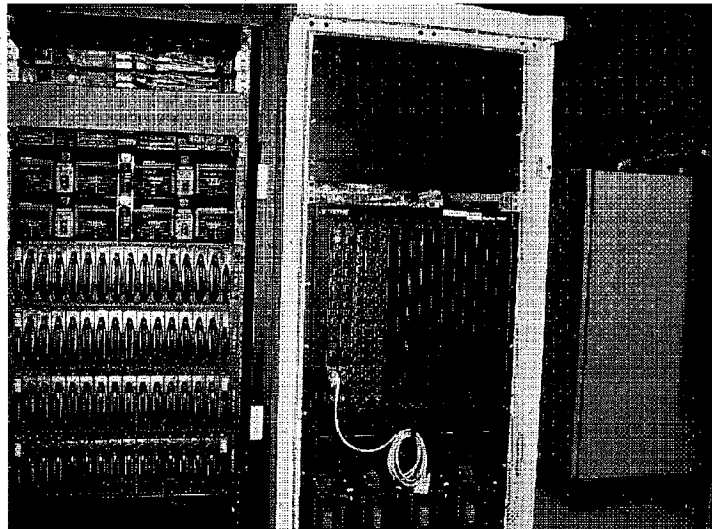
What to do with so much data?

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



One Solution...

Regional
Computer
Forensic
Laboratory





QuickTime™ and a
decompressor
are needed to see this picture.

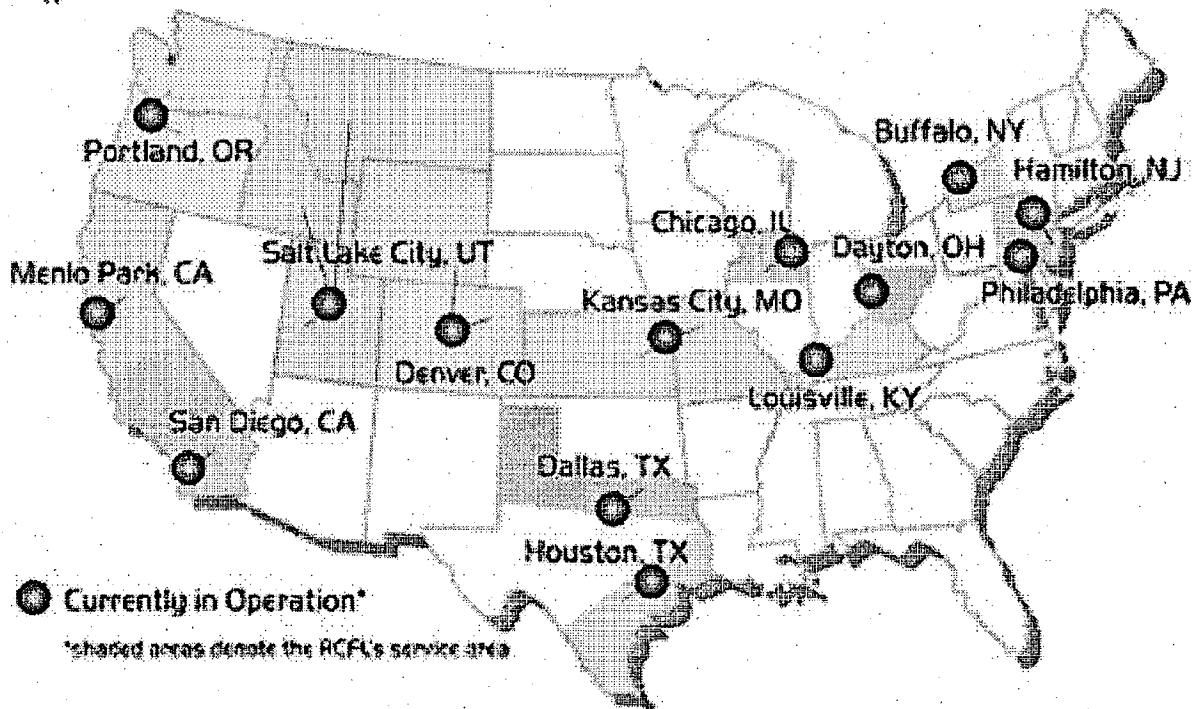


What is the RCFL Program

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



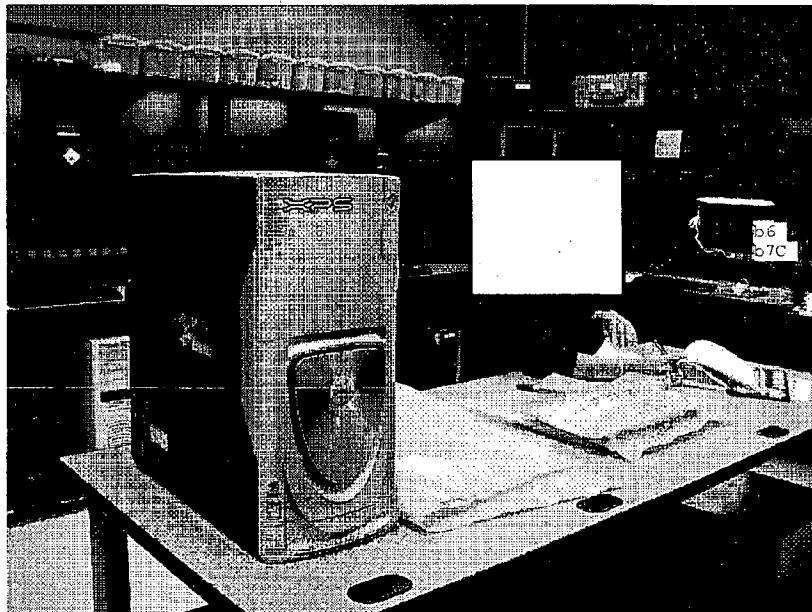
U.S. Digital Evidence Laboratories





What is an RCFL

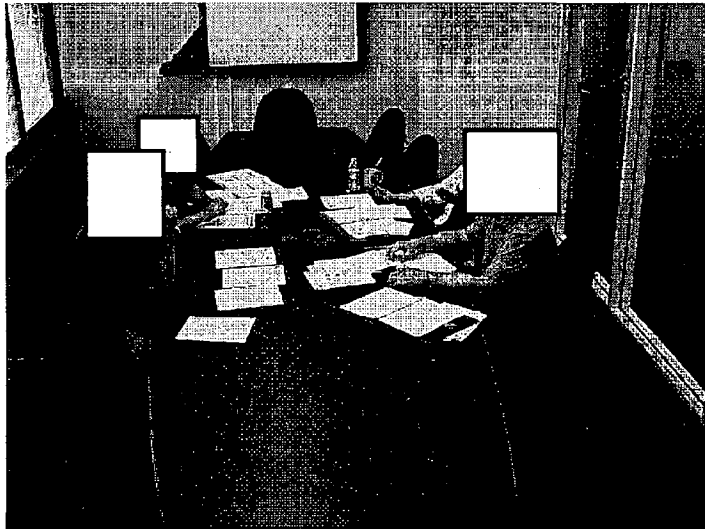
- Single service forensic laboratory devoted entirely to the examination of computer/digital evidence in support of criminal investigations.





What is an RCFL

- A unique law enforcement partnership that promotes quality and strengthens computer forensics.

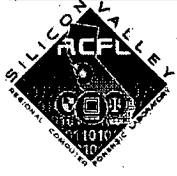


b6
b7C



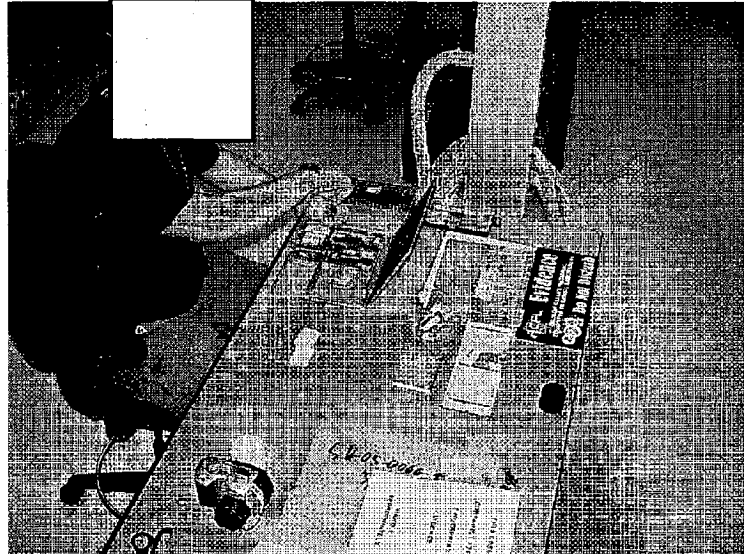
RCFL History

- 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

- 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



b6
b7C



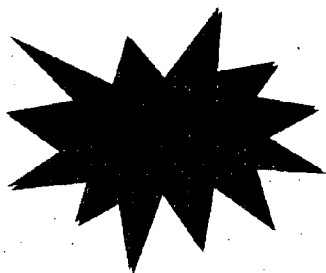
Regional Computer Forensic Laboratory

- 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
-



SVRCFL Personnel Status

- State and Local Commitment
 - Alameda County Sheriff's Office
 - Newark Police Department
 - Oakland Police Department
 - Palo Alto Police Department (position vacant)
 - San Jose Police Department
 - San Mateo County Sheriff's Office
 - Santa Clara County District Attorney's Office
- Federal Commitment
 - Federal Bureau of Investigation
 - RCFL Director
 - (2) Special Agent Forensic Examiners
 - (4) Non-sworn Forensic Examiners
 - (3) Special Agent Forensic Examiner Trainees (part time)
 - Systems Administrator
 - Lab Assistant
 - -----
 - 9 full-time/3 part-time



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

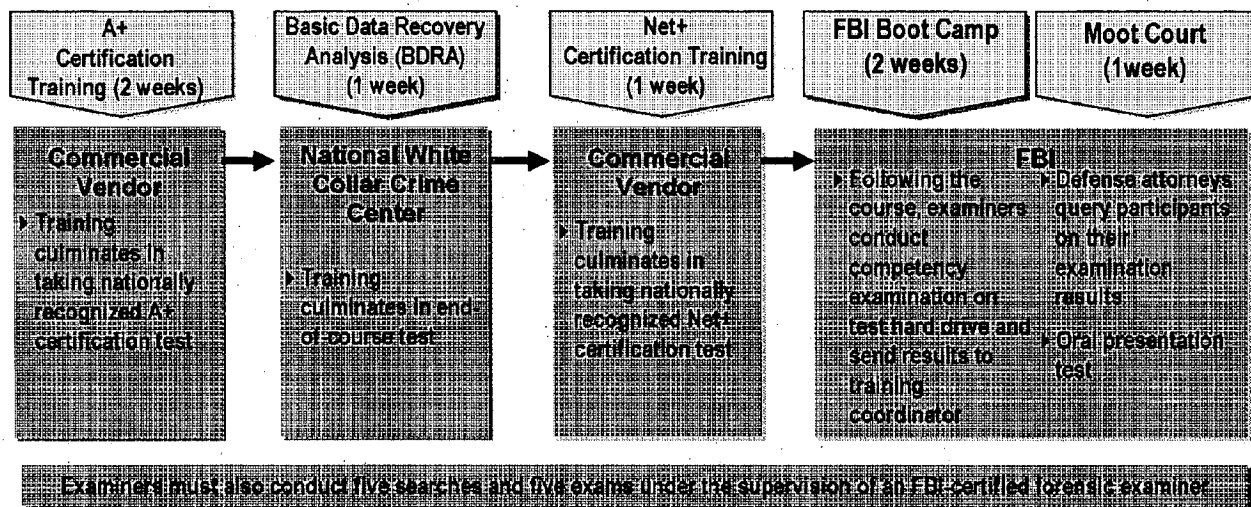


Benefits of Participation

Agency	Examiner	Community
✓ Computer forensic services and standards ✓ Capability ✓ Training ✓ Knowledge and experience	✓ Training ✓ Networking ✓ Knowledge and experience ✓ DOJ Protection	✓ Highest quality service ✓ Crisis response capability ✓ Training to LE officers ✓ Quality law enforcement ✓ National leadership



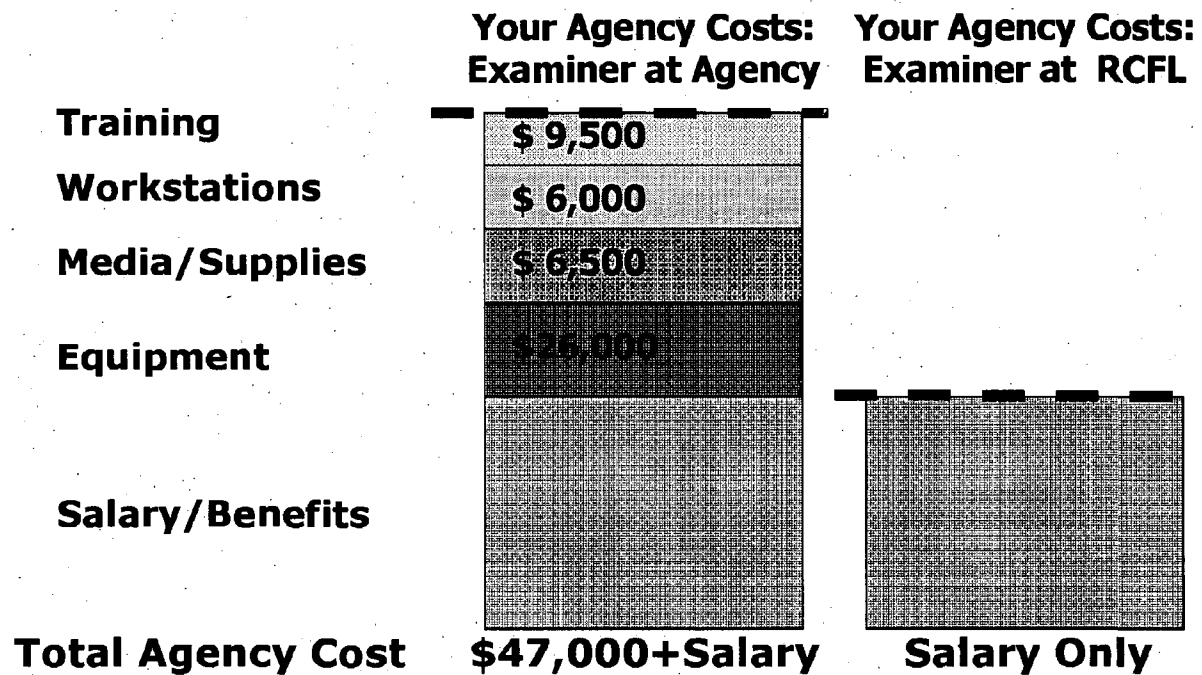
Examiner Training/Certification



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



Examiner Costs





Examiner Costs/Benefit

- Initial training
 - Annual Advanced Training
 - 2 weeks/year minimum
 - New disciplines (Mac/PDA/Cell/Unix)
 - Annual Continuing Education
 - Up to \$5,000 each per year
-



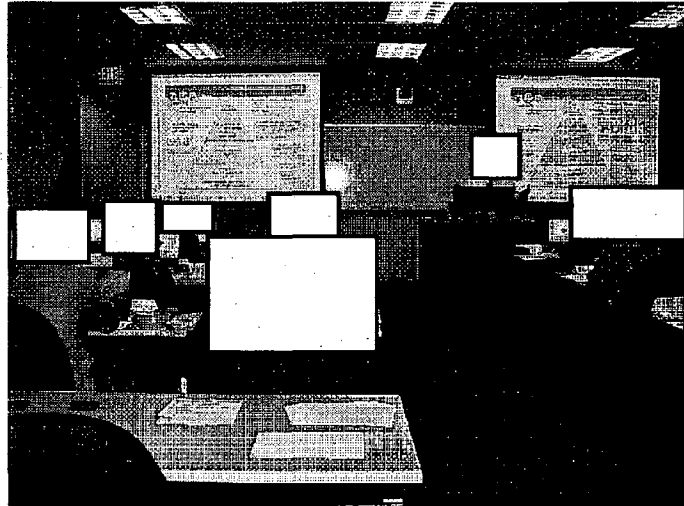
Training

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

www.svrcfl.org for training info

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

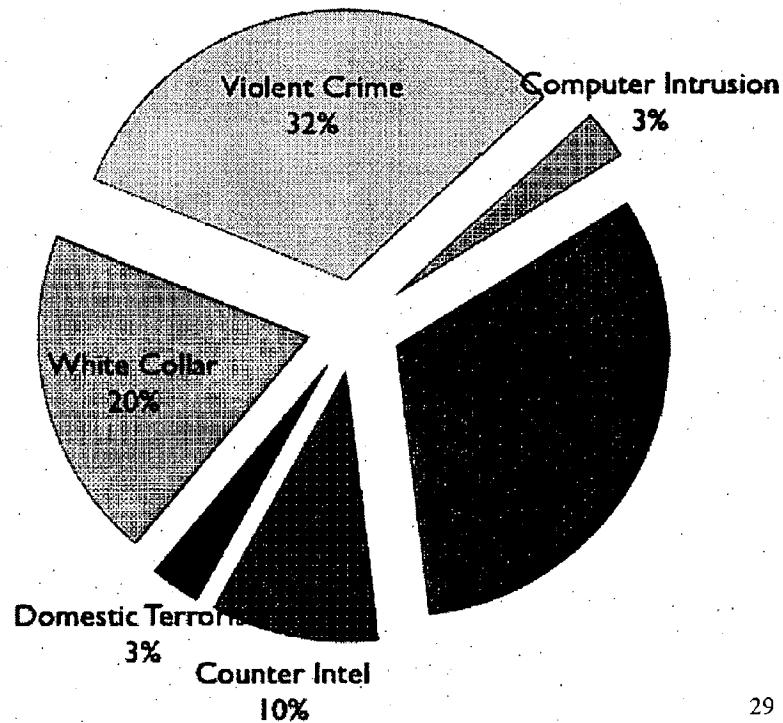
- LAW ENFORCEMENT ONLY





Based on data processed

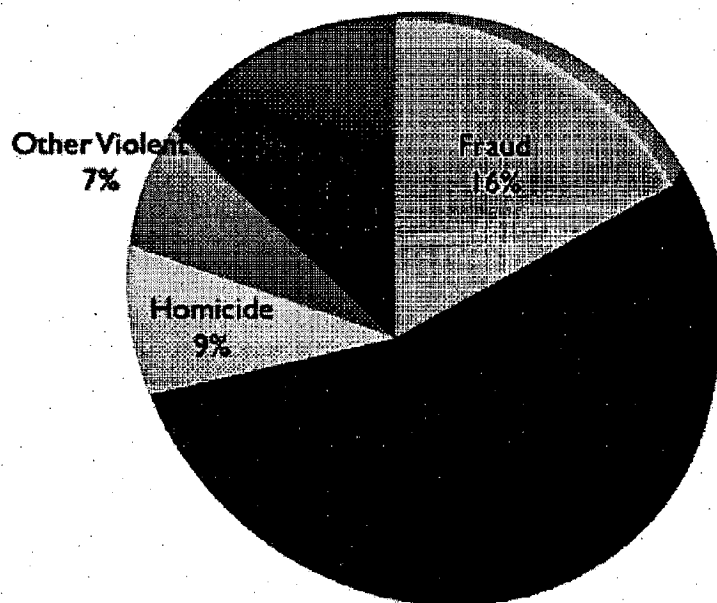
Cases by FBI Program FY2008



29



Cases -- State/Local/Other Fed





Funding

State and Local Provisions

Personnel

FBI Field Office Provisions

Personnel

SVRCFL Provisions '04-'08 \$4.2m (through Congressional Funding)

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



How to Participate

- Must be law enforcement agency in Bay Area
 - Review MOU
 - 2 yr. full time
 - Car + gas*
 - Cell phone*
 - Addendum is drafted
 - Identify Personnel
 - Meet with LEB and vote
-



Memorandum of Understanding

- 2 Year full-time commitment of personnel resource, detailed to the RCFL:
 - Sworn or non-sworn digital forensic examiner
 - DOES NOT require personnel who are trained in the recovery of digital evidence
 - Non-sworn administrative detailee (receptionist, system administrator, evidence technician)
 - Part-time forensic examiner could be considered
- Local Executive Board



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
 - 650.289-3000
 - [REDACTED]@rcfl.gov
 - www.rcfl.gov
 - www.svrclf.net

b6
b7c

b6
b7c