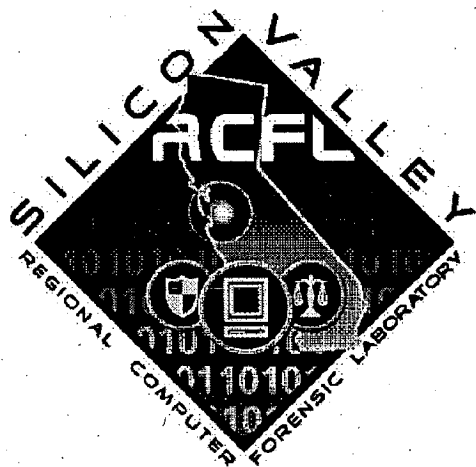




***Supporting Law
Enforcement's Needs in
the Digital Age***

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

www.rcfl.gov
www.svrcfl.net

info@svrcfl.net



Contact Information

- [Redacted]
- [Redacted]
- FBI Supervisory Special Agent

b6
b7C

- [Redacted]
- (650) 289-3000
- 4600 Bohannon Drive #200
- Menlo Park, CA 94025

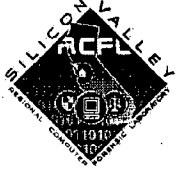
b6
b7C



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)
-

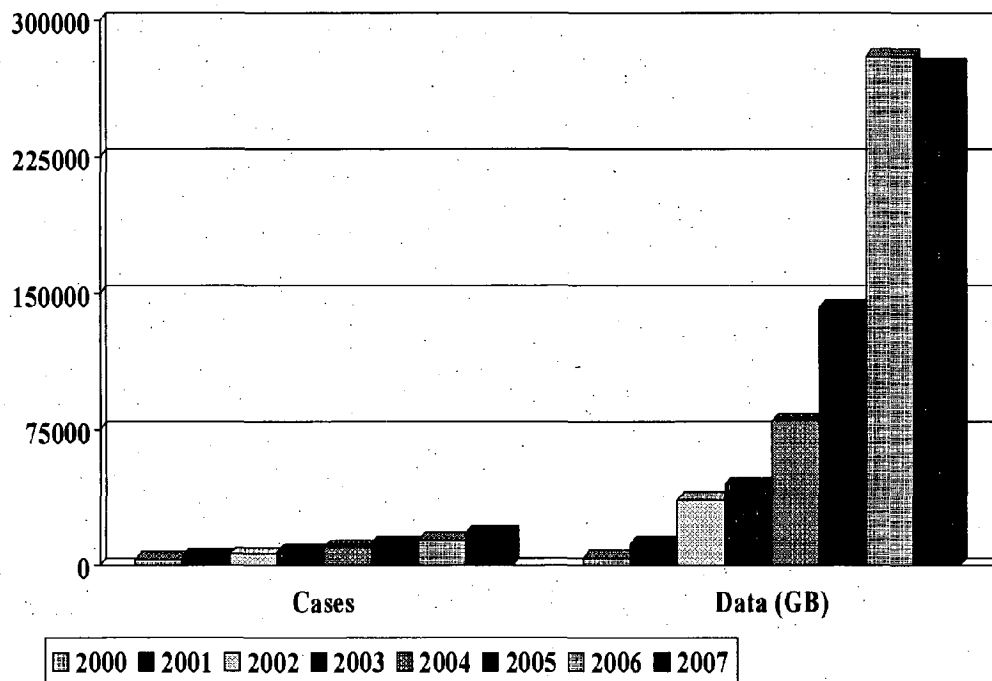


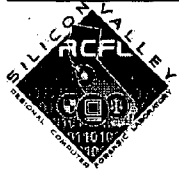
As a Result:

- 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
-



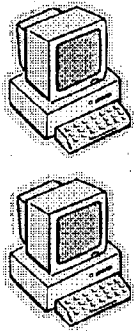
Why do we need RCFLs?



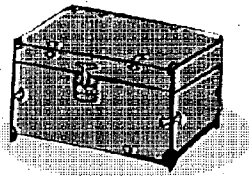


Examples

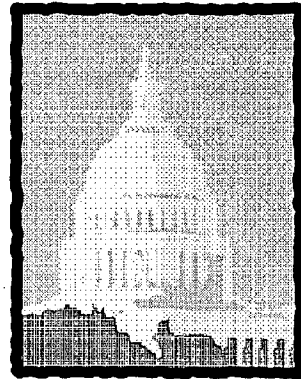
Data Glut



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
-
- Credit: "How much Information?," University of California at Berkeley, 2001, 2003



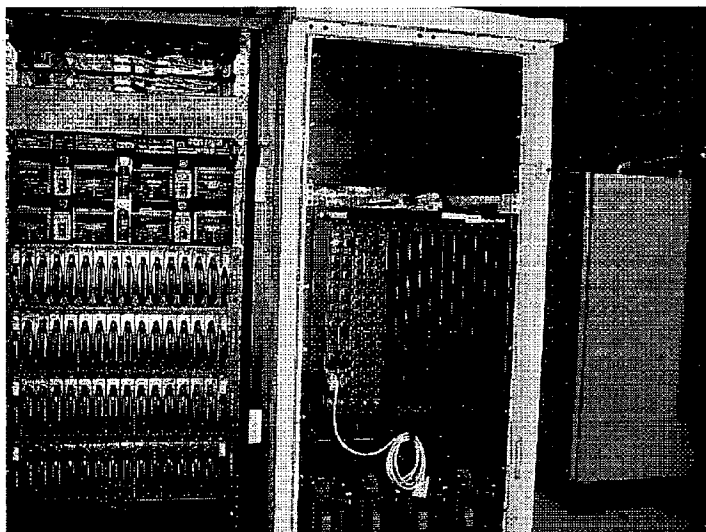
What to do with so much data?

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



One Solution...

Regional
Computer
Forensic
Laboratory



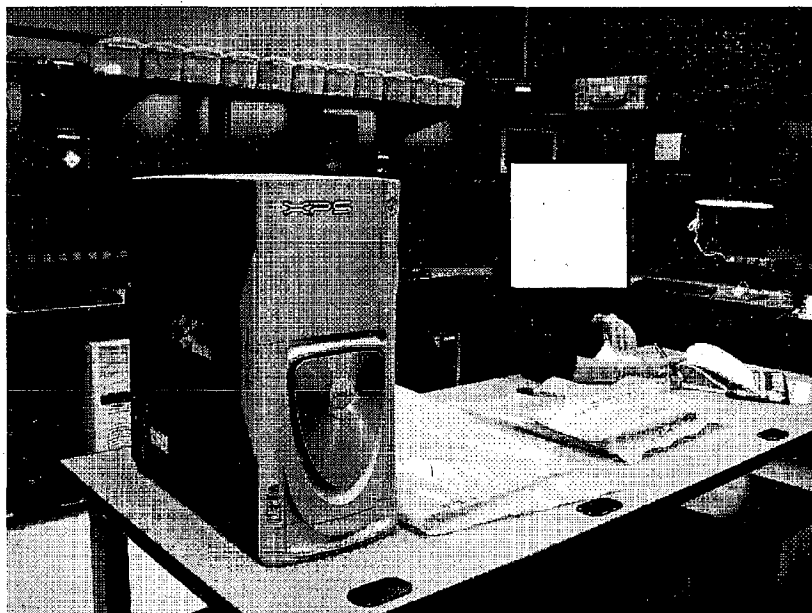
11/30/01 15:45
Domestic Disturbance

b6
b7C



What is an RCFL

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

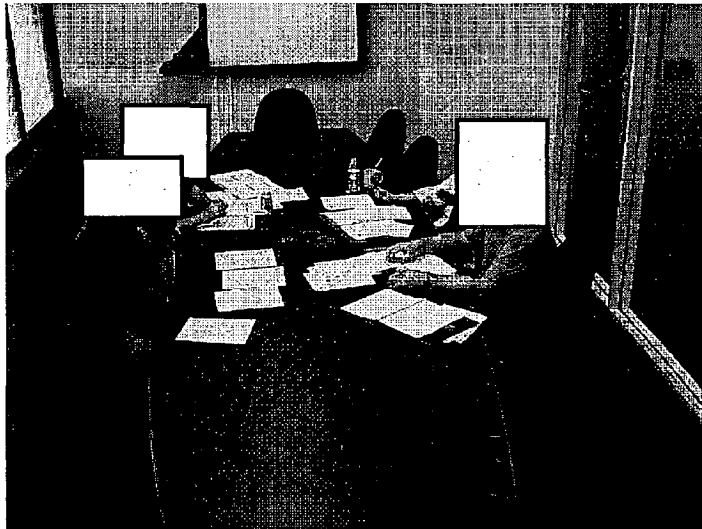


b6
b7c



What is an RCFL

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



b6
b7C

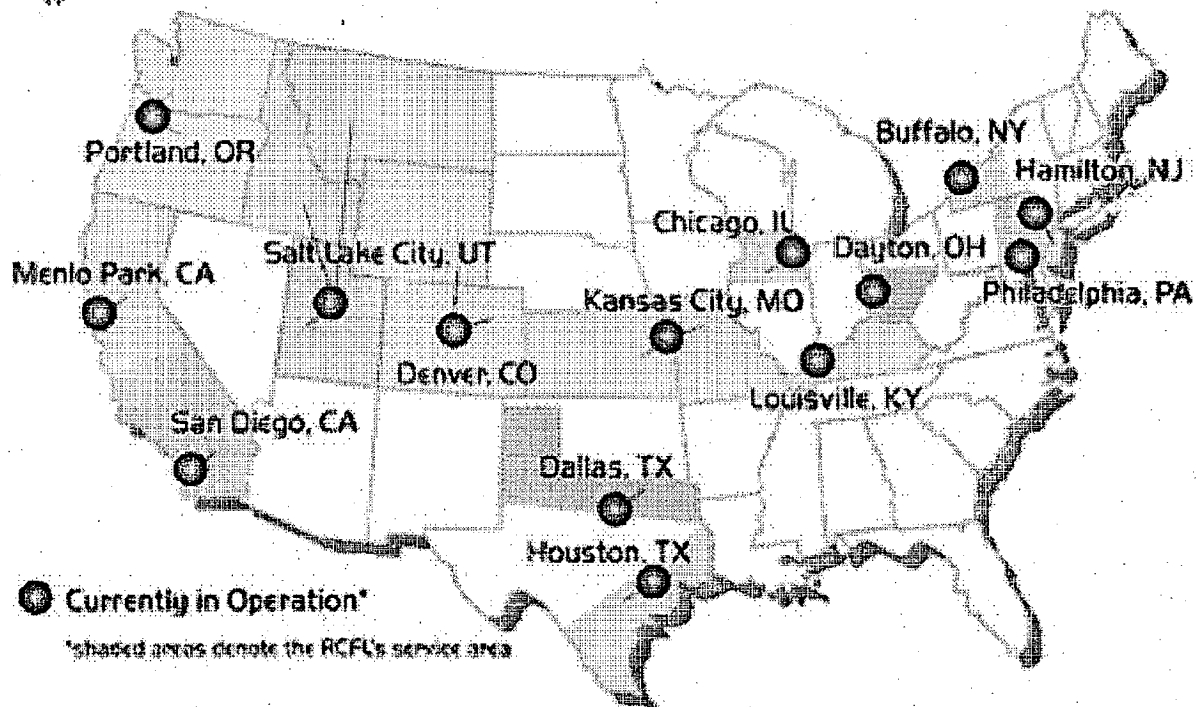


What is the RCFL Program

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



U.S. Digital Evidence Laboratories





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.



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
-



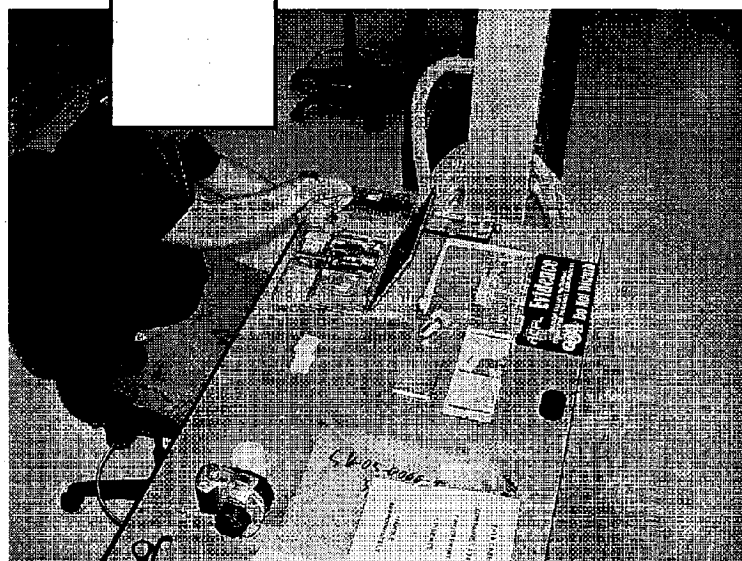
RCFL History

- 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

- 2000 Dallas, TX
- 2003 Chicago
- 2003 Kansas City
- 2003 Silicon Valley

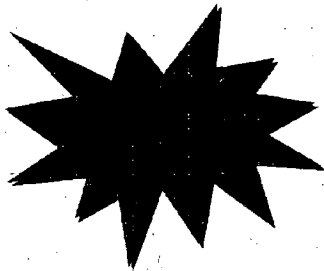


b6
b7c



ASCLD/LAB Accreditation

American Society of Crime Lab Directors/Lab Accreditation Board

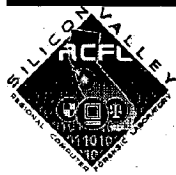


- ✓ Provides an independent, impartial, and objective system for lab operational review
- ✓ Assesses lab quality assurance program including:
 - SOPs and Quality Manual
 - Proficiency testing
 - Continuing education
 - Other programs to help the laboratory give better overall service



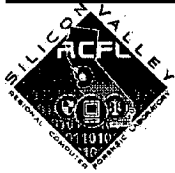
Case Prioritization (LEB/MOU)

- | |
|--|
| 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 |

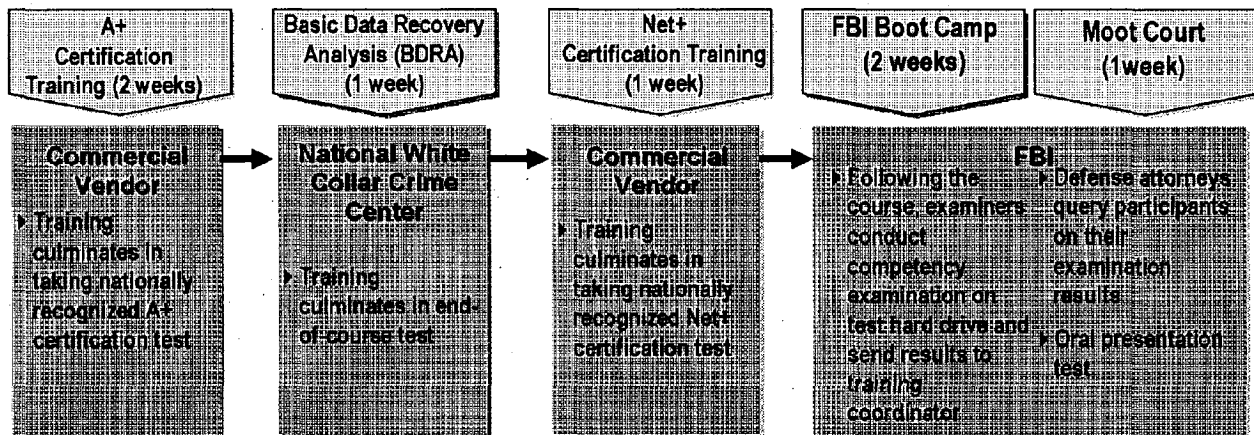


SVRCFL Personnel Status

- 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



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



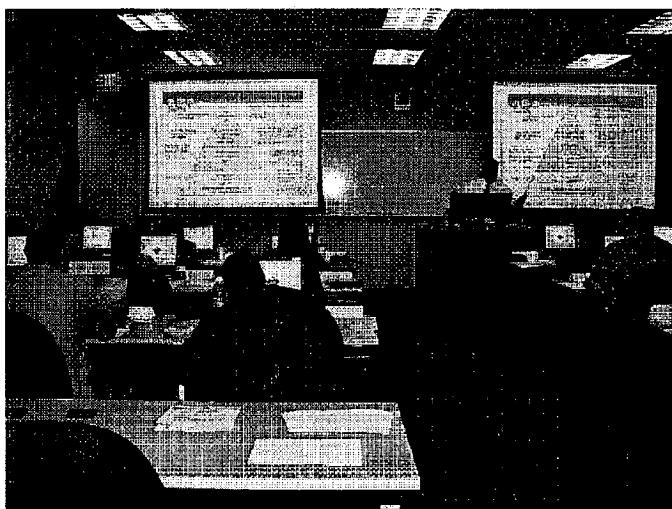
Training

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

www.svrcfl.org for training info

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

- LAW ENFORCEMENT ONLY





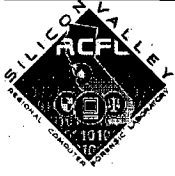
26

b6
b7c



National RCFL "Fun Facts"

- Trained more than 21K LEOs worldwide in last 5 years
- 685 LEAs requested assistance - 89% non-federal
- 15,207 requests for service since 2003
 - 13,500+ Examination requests
 - Almost 3 Petabytes (2,972TB) examined!

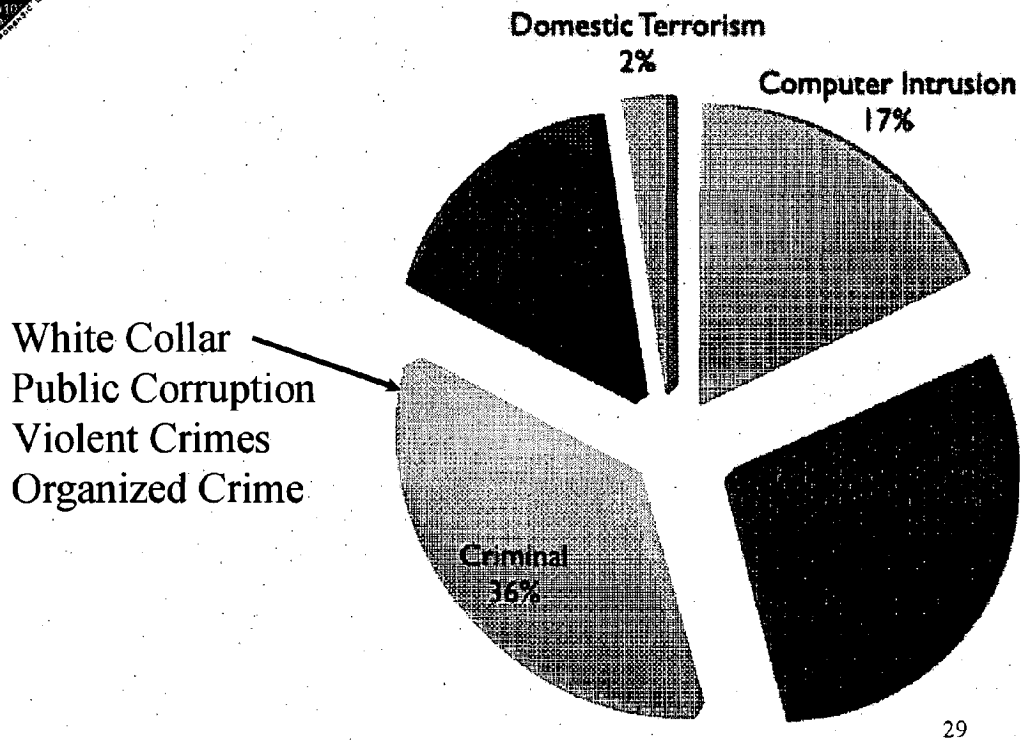


National RCFL "Fun Facts"

- FY2007:
 - 17,378 Hard disks analyzed
 - 11,781 Floppy disks analyzed
 - 1,486 cell phones
 - 37,424 CD's
 - 4,374 DVD's
 - 4,138 everything else
- TOTAL 76,581 pieces of media imaged and processed!!!!

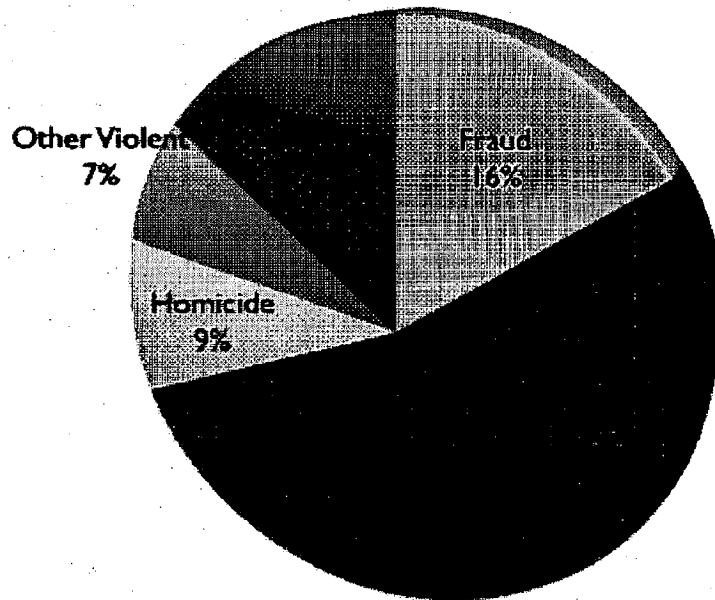


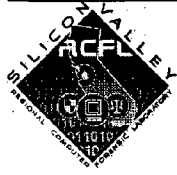
Cases by FBI Program FY2007





2007 -- State/Local/Other Fed



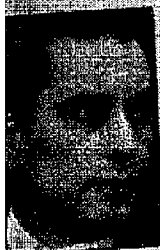


SVRCFL in the News

- Unsung heroes.



Unsung Heroes



Reiser
The computer
programmer
sighed and
hung his head
after being
found guilty of
murder
Monday.

Reiser guilty of killing his wife

JURY CONVICTS
DESPITE NO BODY

By Chris Metinko
Bay Area News Group

32



Ex-teacher linked to more porn

1990年12月15日

[HOME](#)[NEWS](#)[ON THE AIR](#)[VIDEO](#)[AUDIO](#)[EXTRAS](#)[ABOUT US](#)[PARTNERS](#)

Local News

[SHARE](#)

Posted: Thursday, 24 April 2008 10:45AM

SF Couple Accused of Terrorizing Tenants

SAN FRANCISCO (AP) - A landlord couple accused of cutting the supports under a renter's San Francisco apartment are facing felony charges in an alleged campaign to terrorize tenants into leaving.

Prosecutors say software engineer Kip Macy, 33, and real estate agent Nicole Macy, 32, told workers to cut the beams supporting the tenant's floor after he successfully fought eviction in court.

The couple also allegedly shut off his electricity, cut his phone line and had workers saw a hole in his living room floor from below.

Authorities arrested the pair Tuesday and charged them with felony stalking, burglary and



NETWORKWORLD

This story appeared on Network World at
<http://www.networkworld.com/news/2005/091505-berkeley-thief.html>

UC Berkeley recovers stolen laptop with 98,000 names



SFGate.com

[Print This Article](#)

[Back to](#)

Article

SFGate.com

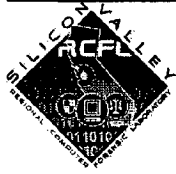
\$50,000 reward in Chiron probe FBI seeking fresh tips on blast suspect

Peter Fimrite, Chronicle Staff Writer

Friday, December 5, 2003



The FBI offered a \$50,000 reward Thursday for information leading to the arrest of Daniel Andreas San Diego, who authorities believe was i
with ties to animal testing



Other Cases

- SK Foods
- Growers Express
- Operation Remaster
 - 2 defendants (37 months)
 - 494,000 counterfeit items including pirated music, movies, software...
 - largest manufacturing case in US involving high-quality counterfeit movies



It's about:

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



For further information:

-
- Regional Computer Forensic Laboratory
 - Silicon Valley
 - 4600 Bohannon Drive
 - Suite 200
 - Menlo Park, CA
 - 650.289-3000
 -
 - www.rcfl.gov
 - www.svrcfl.net

b6
b7c