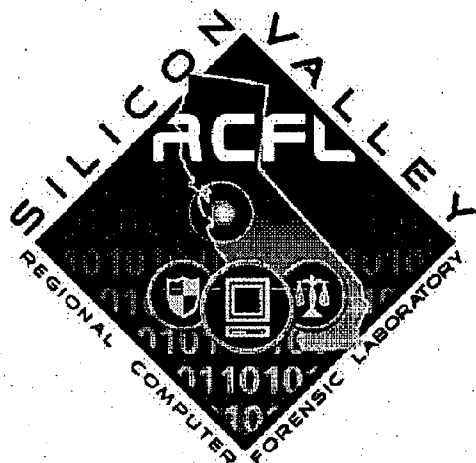




Supporting Law Enforcement's Needs in the Digital Age

SSA [redacted]
[redacted] SVRCFL
[redacted] @svrcfl.net
[redacted]

b6
b7c



Agenda

- What is an RCFL?
 - How do RCFLs help Law Enforcement?
 - RCFL Activities?
 - Where are the RCFLs currently located & being built?
 - Why should Law Enforcement participate?
 - Questions & Discussion
-



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
 - Blackberry

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 5 years
 - Terrorism
 - Counter Intelligence
 - Cyber (Hacking, Trade Secrets)
 - White Collar Crimes
 - Violent Crimes (incl. Sexual Predator)
-



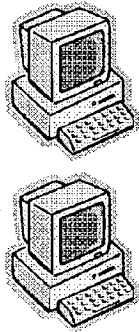
As a Result:

- Traditional Crimes are producing enormous amounts of digital evidence
- Cyber Crimes are producing complex digital evidence
- Law enforcement, at all levels, is unprepared for "data glut"

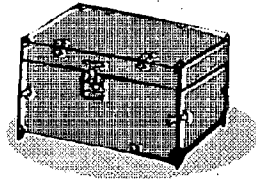


Examples

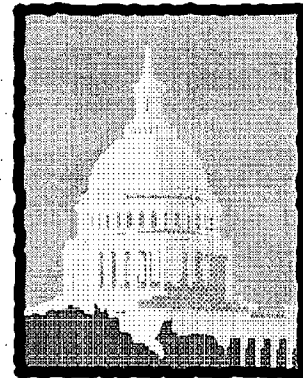
Data Glut



Tradebomb
1993



Okbomb
1995



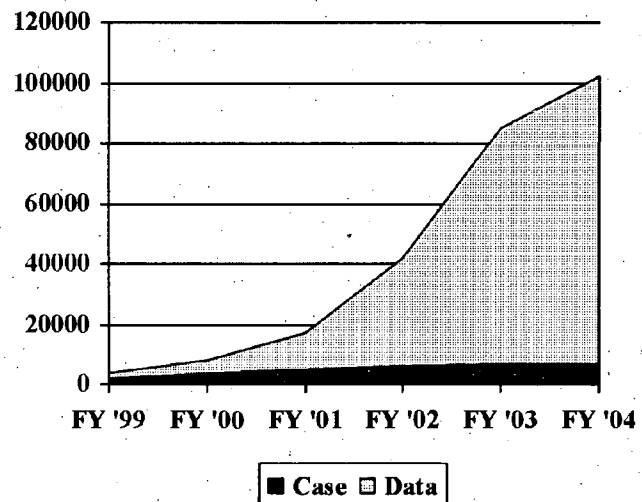
Penttbom
2001 (7.4T)



Why do we need RCFLs?

FBI CART & RCFL Experience

- Case load:
 - FY '99 - 2084 cases
 - FY '00 - 3891 cases
 - FY '01 - 5166 cases
 - FY '02 - 5924 cases
 - FY '03 - 6546 cases
 - 26,000+ Computers!
 - FY '04 - 7000+ cases
- Data examined:
 - FY '99 - 17 terabytes
 - FY '00 - 39 terabytes
 - FY '01 - 119 terabytes
 - FY '02 - 358 terabytes
 - FY '03 - 782 terabytes
 - FY '04 - 950+ terabytes!





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
- 400 terabytes: National Climatic Data Center (NOAA) database

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



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



- Play KRON video



What is Computer Forensics?

- Impartial examination, analysis and presentation of computer evidence
 - Extraction of computer evidence without any alteration of the original material
 - Ability to present the evidence in a court of law by expert witnesses
-

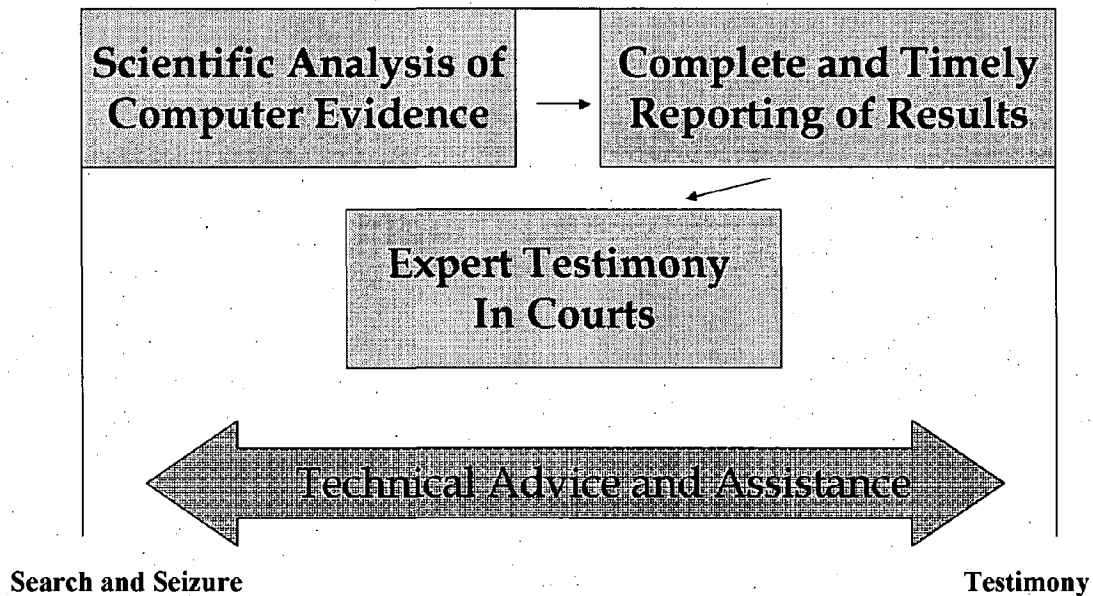


What is an RCFL?

- Single service forensic laboratory devoted entirely to the examination of computer evidence in support of criminal investigations.
 - A unique law enforcement partnership that promotes quality and strengthens computer forensics.
-



RCFL Activities



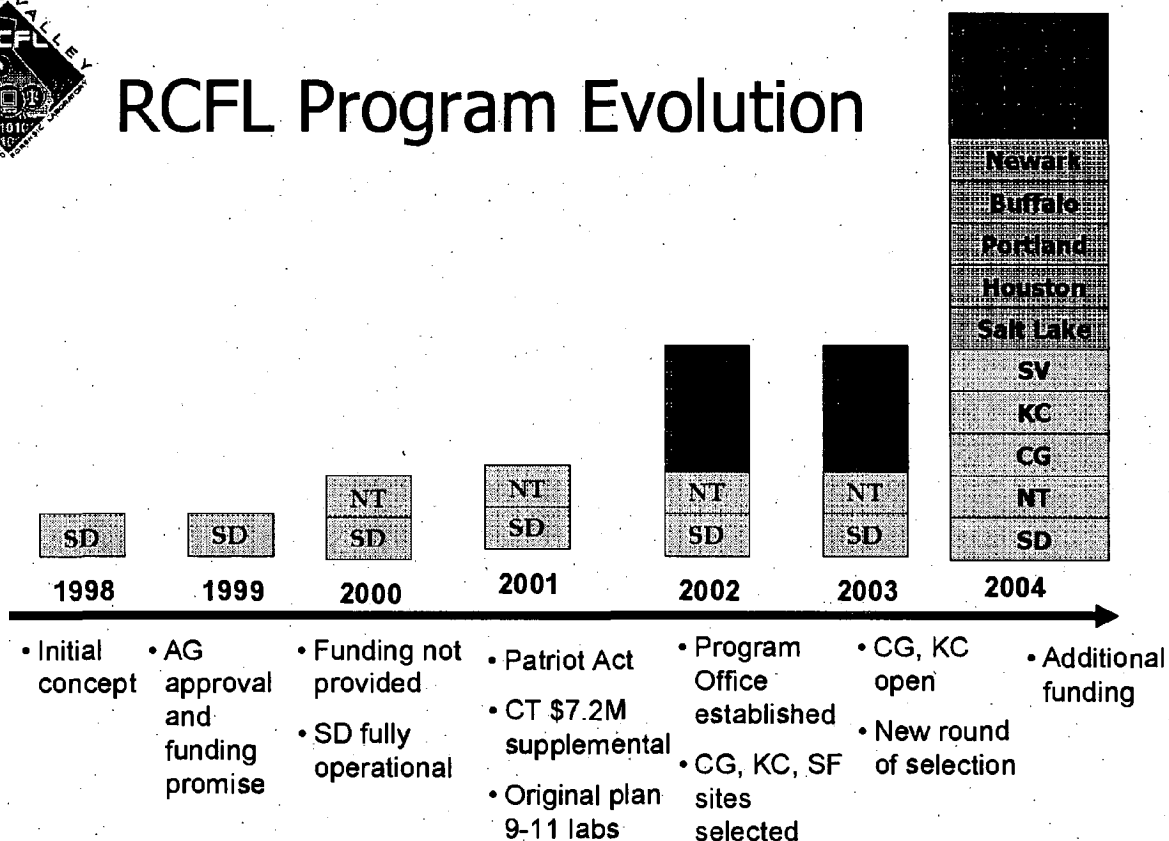


An RCFL is:

- Available to any law enforcement agency in the region it supports
 - Staffed by technically qualified members of the law enforcement (sworn and non-sworn) community in the supported region who are detailed to RCFL from their parent agencies
-

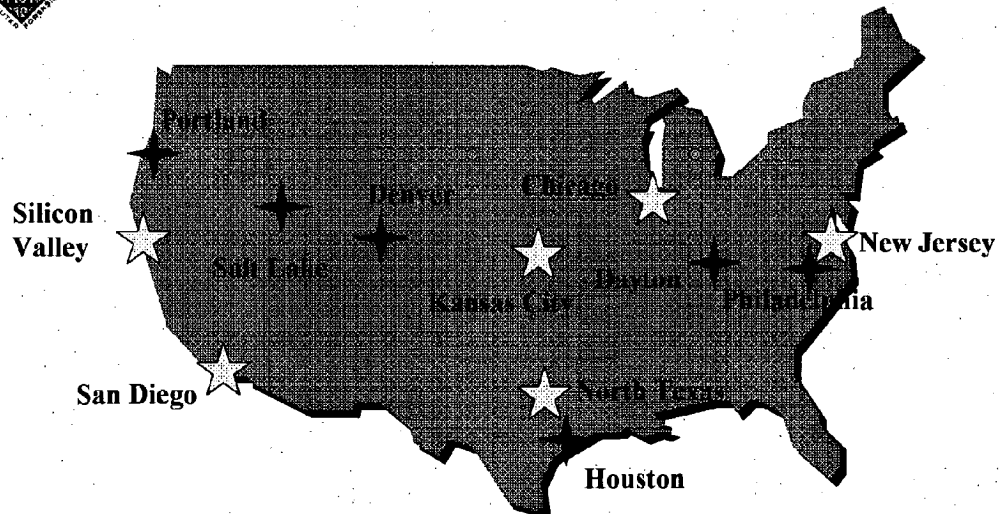


RCFL Program Evolution





Status of National Program



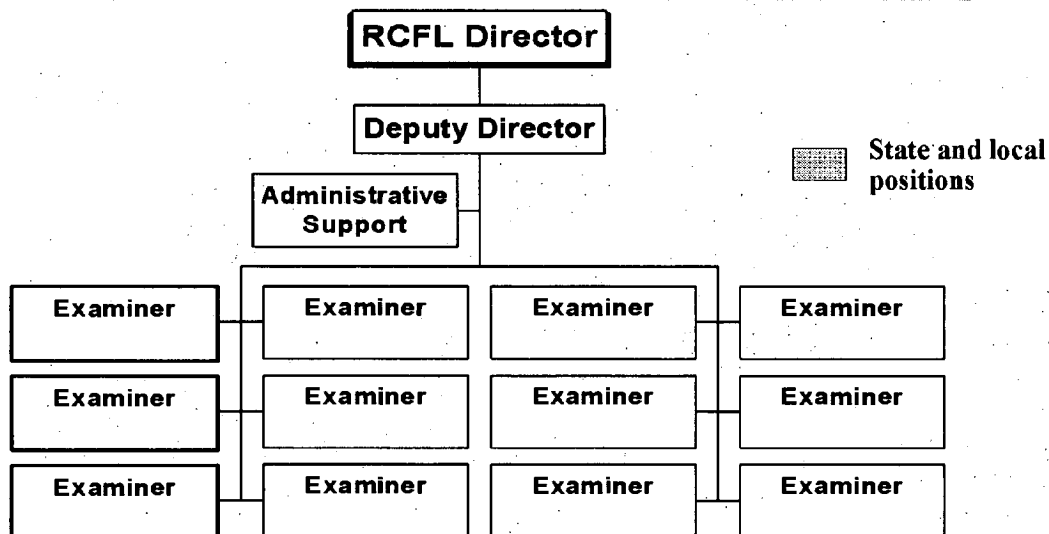


Benefits of Participation

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

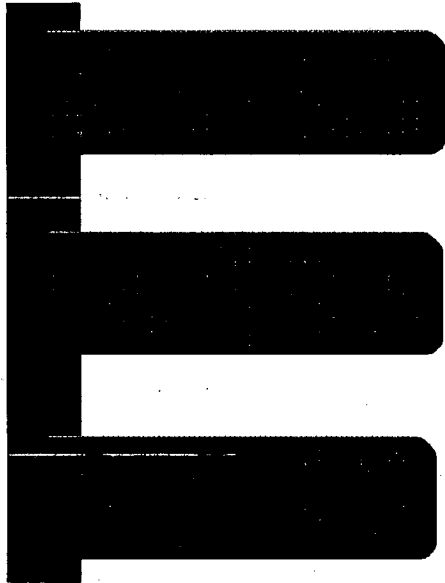


Typical RCFL Organization





RCFL Governance



Represents key stakeholder groups and advises on overarching policy issues

Represents the computer forensic technical community and helps set technical operating standards that will meet American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) and/or other standards

Represent your local participating agencies and provide operational guidance and oversight



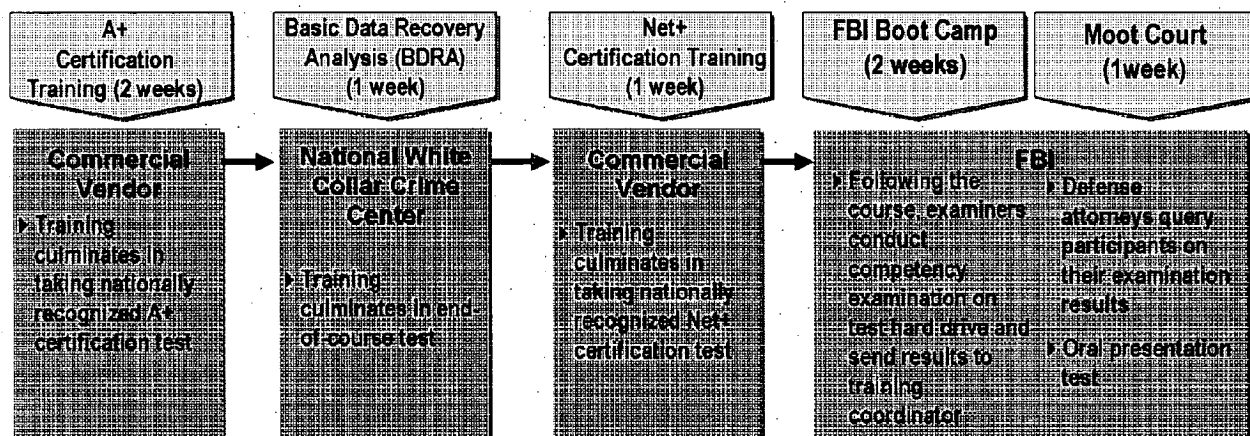
RCFL Accomplishments at a Glance

FY03 Program Accomplishments (2+2 RCFL's)

- ✓ Processed **82.3** Terabytes of data
- ✓ Accepted **1393** requests for service
- ✓ Participated in **196** search and seizure operations
- ✓ Trained **1525** law enforcement personnel
- ✓ Conducted **987** computer forensic examinations
- ✓ Served **924** law enforcement agencies in five states



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

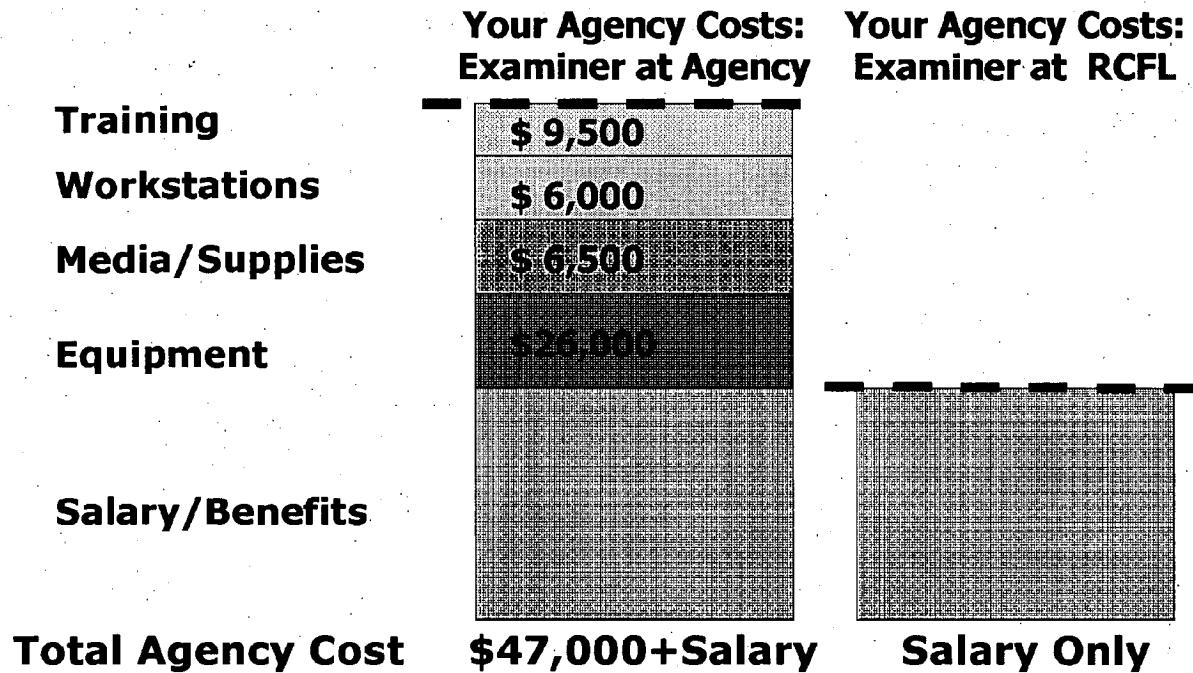


Memorandum of Understanding

- 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
-



Examiner Costs





Total Lab Funding

State and Local Provisions

Personnel

FBI Field Office Provisions

Personnel

SVRCFL Provisions \$2.9m (through Congressional Funding)

Facility Construction	\$929,000
Facility Infrastructure	\$700,000+
Facility Supplies/Furniture	\$140,000+
Facility Lease (annual)	\$580,000
Examiner ▪ Equipment (every 2-3 years) ▪ Training (every year) ▪ Workstations	\$42,000/ examiner
Common Equipment (annual)	\$50,000
Media and Supplies (annual)	\$50,000
Training Room Equipment and Furniture	\$150,000



Personnel Status

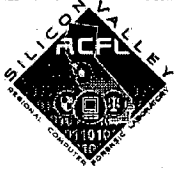
State and Local Partners

- Alameda County Sheriff's Office
 - Palo Alto Police Department
 - San Jose Police Department
 - San Mateo County Sheriff's Office
 - Santa Clara County District Attorney's Office
-



Personnel Status

- **FBI Commitment**
 - Provide SSA for 1st term Director
 - Provide Full-Time Lab Assistant
 - Provide one SA Forensic Examiner
 - Provide 3 IT Forensic Examiners (non-sworn)
-



How does the RCFL work?

- Similar to any crime laboratory
 - Accept computer evidence w/o prior arrangements M-F 8:15am-5:00pm (7am-7pm):
 - Service Request
 - Legal Process
 - Case is opened, prioritized and assigned to an examiner.
 - Examiner contacts investigator within 7 days of receiving the case.
 - Digital evidence is inventoried, preserved, examined and presented to the investigator for analytical review.
 - A final product and report are generated.
 - Evidence is picked up by submitting agency.



Streamline Examination Processes

Forensic Networks



Review Networks



Review Software



Examination Software



Consensual Search
Software



FBI Computer Forensic
Knowledge Base





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 |



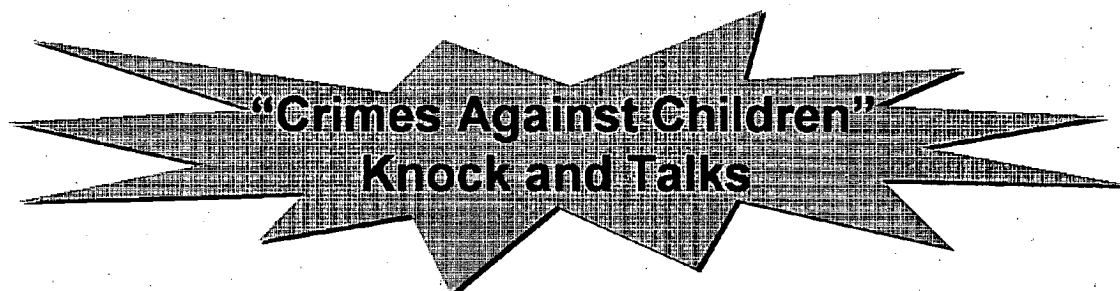
Other benefits of the RCFL

– Classroom and Training (both FBI and S/L)

- Bag and Tag (4 hours)
 - Case Agent (3 days)
 - Image Scan (6 hours)
-
- Classroom available for other cyber/technical courses



Providing Investigator tools "Image Scan"



Boot disk locks
suspect's hard
drive



Investigator
retrieves active
graphics files



- Play ABC 7 Video



It's about:

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



For further information:



b6
b7C

Regional Computer Forensic Laboratory
Silicon Valley

4600 Bohannon Drive
Suite 200
Menlo Park, CA



b6
b7C

@svrcfl.org
www.svrcfl.org