



Fulcrum Financial Inquiry LLP  
888 S. Figueroa Street, Suite 2000  
Los Angeles, CA 90017

(213) 787-4100  
www.fulcrum.com

## **DANIEL RAYMOND NOLTE**

213-787-4148  
dan.nolte@fulcrum.com

### **SUMMARY**

Mr. Nolte has 24 years experience as a system and network administrator in a wide variety of computer systems, programming languages, and networks. He is skilled in computer forensics, web design, application programming, and database applications.

### **EDUCATION AND TRAINING**

Advanced EnCase Training in network intrusion investigations, advanced internet investigations, NTFS file system internals, and cell phone forensics

Microsoft Certified Small Business System Specialist

Postgraduate Certificate in Management Practice for Technical Professionals, UC Irvine

Bachelor of Science, Architecture, Cal Poly SLO, California Architect's License C14889

### **EMPLOYMENT**

Fulcrum Financial Inquiry LLP, Computer Specialist, (2002 to present)  
Computer forensics and investigations (see representative engagements below)

Facility Innovations, Owner and Founder, (1994 to present)  
Contract programming, web design and system/network administration of small business networks.  
Also designed, created, sold, supported, and provided training on the Time and Place Facility Scheduling Software for Microsoft Windows

Ospro/CTG, and Prime Computers (1986 to 1996)  
Provided pre-sales and post-sales technical support

Continental Graphics (1984 to 1986)  
Design Operator and System Administrator

### **REPRESENTATIVE INVESTIGATIONS**

- Multiple criminal investigations in which computerized evidence was relevant. Provided in-court testimony when necessary. The cases typically include issues of intentional vs. unintentional possessions, search history, viewing history, file locations and characteristics, and the analysis of removable media.

- Multiple engagements involving the authentication and/or origination of electronic data. The underlying allegations generally involve (i) proving or disproving a claimed alibi, or (ii) understanding the source of claimed evidence.
- Multiple investigations of computerized files, including metadata, file versions, and date/time stamping. These engagements generally involve either allegations of theft of trade secrets by former employees, copyright infringement, or other intellectual property allegations.
- Multiple investigations of seized hard disk as to whether the alleged files appeared on the disk, as well as whether the broad categories of images or other data found on the system were consistent with the accusations involved. These engagements generally involve allegations of inappropriate conduct by employees during office hours.
- Conducted a detailed digital analysis of an audiotape on the question of whether it had been edited together from its separate parts.
- Electronic data discovery in discovery, including recovery and conversion of data obtained from opposing parties.

## **COURT TESTIMONIES**

Because most investigations report ascertainable facts involving digital evidence, the results of the investigation (particularly civil investigations) are ultimately not disputed. The following listing lists only projects where court testimony was provided. This list does not include written reports, percipient deposition testimony regarding investigation results, declarations, administrative appearances, or appearances as a special referee/master.

	Case Allegations	Testimony Description
1	Financial Fraud	Examination of defendant's computer and examination of e-mail records from defendant's computer and on-line accounts.
2	Possession of Child Pornography	Examined image of defendant's hard disk to obtain additional information regarding the suspect images. Testimony on the nature of peer-to-peer file sharing in relation to what could be considered intentional or unintentional possession in regards to the peer-to-peer software being used.
3	Possession of Child Pornography	Examined image of defendant's hard disk to find additional information regarding the suspect images. Testified on the nature of thumbnail images, the function of the temporary internet files folder, and the circumstances that might result in thumbnail images unintentionally appearing in temporary internet files.
4	Sexual Conduct with a Minor	Much of the evidence in the case involved messages sent to and from a social networking site. Defendant claimed that the charges were being orchestrated by defendant's estranged ex-wife. Testimony was prepared on the nature of the social networking contacts and of the ex-wife's computer activities.