# Working with the Computer Forensic Examiner

*This document was prepared by Deputy District Attorney Michael S. Groch, San Diego County District Attorney's Office.*

Working with a computer forensic examiner requires all of the prosecutorial skills needed to work with experts in general — and a few additional ones. You must understand what your examiner can and cannot do. You must be sure that you understand the lingo the examiner will use and how to communicate that to the jury. Also, compared to other fields, computer forensics is relatively new. This presents many areas for a capable defense attorney to attack. These and many other issues make presenting digital evidence and working with a forensic examiner a challenging task.

This expanded outline is an attempt to highlight some of the issues that you may encounter and how to handle them. Also contained on this CD-ROM are many examples of direct examinations conducted of forensic experts. They are not presented as "model" examinations, but rather as samples from which you can obtain ideas of how to approach your examination. If you run into difficulties or want any kind of assistance from a prosecutor who has handled volumes of digital evidence, be sure to contact a prosecutor from one of the five regional high-tech crime task forces in California. They can assist you or direct you toward additional resources:

| | |
|---|---|
| **Sacramento Valley Hi-Tech Crimes Task Force** | 916-874-3002<br>www.sachitechcops.org |
| **Northern California Computer Crimes Task Force (NC3TF)** | 707-253-4500<br>www.northbayheat.org |
| **Rapid Allied Enforcement Computer Team (REACT)** | 408-998-5633<br>http://reacttf.org |
| **Southern California High Tech Task Force (SCHTFF)** | 562-345-4260 |
| **Computer and Technology Crime High-tech Response Team (CATCH)** | 619-531-3660<br>www.catchteam.org |

Like many forensic laboratories, computer forensic laboratories are laboring under a huge caseload and limited resources. This requires you to submit the computer for examination — as soon as possible — and to communicate with the examiner as early in the process as you can.

Time and resources may only permit a single forensic examination, in which case you need to be sure the examiner is looking for all of the evidence that you need from the beginning. You should participate in the selection of search terms and the scope of the forensic request. Often, a computer is submitted for examination upon its seizure very early on in a case. At that point, the investigator submitting the lab request may not have all of the facts that you, the prosecutor, have when you get the case. You may also have different needs as you evaluate the case from your prosecutorial perspective. Since you may only get "one bite at the apple," be sure the apple you need is the one you get.

## I. Pre-Testimony Meeting

- **ABSOLUTELY ESSENTIAL**

- **Make your case personal to the examiner**
  - — Meeting ensures the examiner will provide what you need
  - — Meeting shows your interest and dedication
  - — Meeting leaves time for follow-up work

- **Review lab report and notes**
  - — Is everything in discovery? Have lab notes been discovered?
  - — Sufficient inculpatory and exculpatory search strings?
    - "My roommate is the culprit"
    - Be sure search strings for names of suspects you want to exclude are included

- **Able to block anticipated defenses?**
  - — "A hacker put those images on my computer"
    - If you believe this may be a defense tactic, be sure your examination request includes a request to look for evidence of Trojan Horses or back doors on the computer. The location of files (plain sight or concealed), as well as file creation and modification dates, becomes particularly important.

- **Extent of expert's opinion**
  - — Narrow limits scope of voir dire
  - — Narrow limits scope of cross-examination
  - — Narrow limits of irrelevant cross-examination

  Tailor the scope of your expert's opinion as tightly as you can for the above-listed reasons. If your expert is testifying about facts from what he/she observed during an examination and is not offering an opinion, be sure the scope of voir dire and cross-examination is likewise limited.

- **Can the expert go as far as you want/need?**
  Usually an expert cannot put a defendant behind the keyboard. Rather than offering the opinion that defendant "X" sent a threatening message from a

computer he examined, the expert may need to limit his opinion to this: that a message was sent from a particular computer and, further, he found evidence that defendant "X's" name was found in the registry file 455 times and was the default and only logon name. You'll need to argue the facts that the defendant was the one who sent the message. The same is true with a computer filled with child pornography images. Your expert will not opine that defendant "X" downloaded the pictures. Rather, the expert will say the images were found on a computer in which "X" appeared to be the primary user.

- **Reasons for inconclusive results / areas not checked**
  With hard drive sizes typically being at least 40 gigabytes, a typical examination will be a targeted search for specific items and specific locations checked. However, much of the contents of the hard drive, although searched, will not be viewed. You can expect that your examiner will not do a folder by folder search. You need to cover this in your examination if the defense makes an issue out of it and tries to portray your examiner as doing a biased or incomplete examination.

- **Review exhibits you want to use with expert**
  Digital evidence and computer forensics can be very challenging issues for a jury to understand. You must use exhibits to make the concepts real for the jury. If deleted files are a key piece of evidence, be sure your examiner has demonstrative exhibits to explain the process. If the expert does not have any, either make one or purchase one. A resource that sells very good exhibits about unallocated space, deleted files, hash values, etc., is New Technologies at: **www.forensic-intl.com**. You also want to consider asking your examiner for "screen shots" that show the way key pieces of evidence appeared to him during the examination. No matter what you come up with, be sure you review them with your examiner before presenting them to the examiner in court.

## II. Establishing Qualifications

- **New field versus new branch of investigative expertise**
  — New branch incorporates prior police training

- **Résumé / Curriculum vitae (CV)**
  Get your expert's résumé / CV well in advance to familiarize yourself with your expert's level of knowledge and comply with discovery requirements

- **Address degree issue**
  Discuss with examiner whether he has a bachelor's degree in computer science. If not, discuss why it is unnecessary for forensic examinations.

- **Make sure all of these areas are covered in your expert's résumé or CV:**
  — Profession and Position

— Education
  - Formal (degrees and certificates)
  - Informal (seminars and training sessions)
— Work Experience
— Teaching Experience
  - Number of presentations
— Publications
— Honors and Awards
— Memberships and Associations
— Prior Testimony or qualification
— Number of affidavits (if new)

## III. Approach on Expert Direct

- **Avoid technical jargon and low-level details of examination**
  — Avoid bits, bytes, and nibbles
  — Let the defense bore the jury!

- **Get to the results ASAP, then go back and show process**
  For example, "Mr. Expert, did you form an opinion as to whether a person used this particular computer to send the threatening message at issue? What is the basis of that opinion?"

- **Take expert through general methodology, emphasizing**:
  — Work is done on copy
  — Reliability (hash values, write block, etc.)
  — Wide use of forensic software
  — Independent testing of forensic software
  — Peer review of examiner's findings by other experts

- **Re-examination**
  You *must* elicit from your expert that original, still pristine, and additional images can be made for re-examination by "other" examiners

## IV. The Hardware and Software is *not* on trial

- **You don't need to show how software or hardware works**

- **Just show that it is regularly relied upon**

- **Witness doesn't have to completely understand how things work, just how to use them**

- ***People v. Lugashi (1988) 205 Cal.App.3d 632***

## V. Cross of Defense Expert: Approach

- **Get concessions first**
  - — Hash value
  - — Methodology (working off of copy)
  - — Date stamping and OS
  - — Etc.

- **Expert had copy available**
  - — Looked and found the same thing
  - — Didn't look, but could have

- **Send defense expert all materials in advance**
  - — This ensures that the expert considers all of the evidence, not just the stuff the defense likes

### A. Cross of Defense Expert: Expertise

- **Expert is not a *forensic* expert**
  - — Analogize to medical field
  - — System Administrator job is to keep system running, not to conduct examinations
  - — Programmer skills not used in forensic exam
  - — Expert has no experience as an investigator

### B. Cross of Defense Expert: Résumé

- **Demand résumé / CV in advance**
  - — Find the exaggerations / lies in the résumé
  - — Get ethics/standards from professional groups they belong to
  - — If published, get articles!
  - — Search newsgroups and listings for postings