



Q3 eNewsletter 2007 CRITICAL CHECKLIST

Protect your firm from being fleeced by a computer forensics expert.

You need to take precautions and proactively protect your clients and firm from being fleeced by a computer forensics "expert." The information you get from an expert will need to stand up under the watchful, critical (and not necessarily technically savvy) eyes of the judge, opposing counsel, opposing expert, and the jury.

At first glance, a computer forensics expert may pass your litmus test of being competitively priced with hourly billing rates. However, there may be a disastrous "quality deficiency" when comparing the end result in services performed, total hours billed, and evidence produced and sworn to as fact.

Addressing all of the areas in a one-page at-a-glance overview is not possible. However, providing you with a quick reference chart and some critical pointers may save your firm and your clients from being fleeced by a computer geek passing their firm off as "experts" in the field!

Step 1

Ask for and check professional references. (Call and actually talk to the references!)

- a. Question: Were you happy with their work?
- b. Question: Would you hire them again? Why? Why not?
- c. Have you worked with other computer forensics experts? Who? When?
- d. How does this expert compare to your previous computer forensics expert?
- e. How did this expert and their work product impact your case?

Step 2

Ask for a rate sheet, average time to complete tasks, or a range of time to complete each task. Some experts will use a standard flat rate for common tasks, which is also reasonable.

Common Computer Forensics Tasks	Approximate Time Required*
1. Forensic quality image of hard drive	40 - 200 minutes per 100 GB (depending on size and age of hard drive)
2. Duplicate set of hard drive image files (a copy of the raw material)	30-60 minutes per 100 GB
3. Keyword search of image	1-4 hours for 10 keywords on a 100 GB drive (varies based on size of drive, how full the drive is, and number of keywords, and does not include time required to analyze hits)
4. Extract active files, recover deleted files, create file listing, and provide copy on optical or magnetic media	1-2 hours

* These are approximate times. Many variables can affect these tasks, but if you're dealing with a healthy drive, the time should not vary from these ranges too much.

Berryhill Computer Forensics
 P.O. Box 1674
 Benicia, CA 94510
 P 707-745-1405
 P 888-745-1405
 F 707-780-8913
 info@computerforensics.com

FREE *d³* Quarterly eNewsletter
due digital diligence

www.computerforensics.com



Step 3

Ask for details about the analysts who will actually be working on your case. Keep in mind that data recovery expertise is not the same thing as forensic analysis expertise. Computer forensics is the acquisition, analysis and presentation of computer evidence, and a good expert must be skilled in all three of these areas.

- a. **Question:** How many analysts will be used for the job, and what are their qualifications and experience? (Some experts may tout an alphabet soup of certifications as qualification, but keep in mind that there are no standard certifications or requirements in this field. That's what makes item #1 above so important.)
- b. **Question:** Will the analyst(s) working on your case be available during the analysis phase to discuss the results and help you determine whether further analysis would be helpful?
- c. **Question:** If this matter goes to court, will the person testifying be the one who actually did the work?

For every finding presented by the expert, demand the facts to support the conclusion. It is valid for an expert to express opinions, but they must be supported by facts. The expert should be able to explain the facts and conclusions in terms a jury can understand. It won't do your case any good if the expert only uses "geek speak."

Determine the types of data that might have to be disclosed, possibly including: E-mail, Documents, Spreadsheets, Databases, Pictures/Video, Log files, Reconstructed data of any type from deleted or unallocated space

Determine which users within the client's organization might be considered custodians or creators of items to be disclosed.

###

Berryhill Computer Forensics
P.O. Box 1674
Benicia, CA 94510
P 707-745-1405
P 888-745-1405
F 707-780-8913
info@computerforensics.com

FREE *d*³ Quarterly eNewsletter
due digital diligence

www.computerforensics.com