



Q2 eNewsletter 2007 CRITICAL CHECKLIST

Successful Email Recovery

Email can be found in several places: the sending computer, the receiving computer, any number of servers in between the two, or archived in a backup. The sending or receiving computer could be a handheld device including a Personal Digital Assistant (PDA) or a cellular phone.

The first step in a successful email recovery is to identify, remove from service, and secure as many of these items (computers, PDAs, cellular phones, etc) as soon as possible.

The second step is to have the computer(s) examined by someone with computer forensics experience, who is using proper forensic tools. The tools used in computer forensics are highly specialized and ensure that no changes are made to the original evidence. Involving your IT department may potentially destroy evidence.

The simple act of powering up a computer alters critical information. A computer forensic expert will make an image copy of a hard drive, and all analysis will be executed on the imaged copy, not on the original computer. Imaging a hard drive requires using highly technical computer forensics equipment, which is significantly different from having your IT department copy files from a computer hard drive onto a CD.

Copies of emails are often found in the active file structure, and don't need to be pulled out of deleted space. However, there are plenty of complex challenges in email recovery. With a variety of email systems and different software programs to access email, all email files may need to be handled differently. If email has been deleted from a computer, it may not be recoverable from that specific computer, which is why step one must be a top priority and your first critical action.

Step 1

Identify, Remove From Service & Secure Computers

- a. Sending computer & Email server
- b. Receiving computer & Email server
- c. Archived backups
- d. PDAs (e.g. Palm, Blackberry)
- e. Cellular phones

Step 2

Secure Expert Examination

- a. Utilize an experienced computer forensic expert
- b. Demand the use of proper forensics tools
- c. IT departments can damage critical evidence

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



Step 3

Identify Challenges

- a. Variety of email systems
- b. Variety of email software clients
- c. Deleted email may not be recoverable, but may be located on server or backup

Step 4

Isolate & Present Discoverable Information

- a. Dates
- b. Users
- c. Attachments
- d. Forgeries

What kind of information can be discovered about email? Potentially, a lot, including sender, recipient, date sent and received, attachments, and when it was read. Recovering deleted emails is possible. However emails can be forged. A savvy computer user can alter case-critical email information. Therefore, an expert must evaluate it to determine how reliable it is.

If your interest is in protecting your firm, your clients, or settling a case out of court, get a computer forensic expert involved early; it will make your case. Approximately ninety-five percent of the cases we have been involved with have settled out-of-court. I recommend making the call early.

###

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