

# How computer forensics can help your church

By Jim Harmening

It is important to know and understand how a church uses its computer system. Tasks such as writing checks, tracking e-mail and writing correspondence leaves an electronic trail. There needs to be a distinction about who owns this data and whether or not it is public or private information. With the explosion of the information age you should be prepared for what happens after a church worker leaves, whether on good terms or bad.

The more automated and ingrained we become with our technology, the more we will need to find out what happened after the fact. Computer forensics is more of an art than a science and can be used to look at what went on in a computer, even if the information appears to be erased.

## Computer forensics can be used to look at what went on in a computer, even if the information appears to be erased.

Computer forensic programs have the ability to review data in "deleted" sections on the computer hard drive. It also can scan file slack (the parts of a file that are not in use, but may contain remnants of "old" data). There are many log files, printer caches, Internet temporary files and more. A computer forensic examiner has many places to look, but the real key is giving the examiner the right detective work up front.

### A good examiner

For example, if you want to make sure a staff member is not dispersing Social Security numbers, you need to tell the examiner, so the examiner can search for 9 digit numbers, or a series of any number in the following format ###-##-#### (where the # represents any number).

For graphic files, there are many ways to hide what you are doing or ways to encrypt the image files. A good computer forensic

examiner may not know the encryption key, but may be able to use an alternative key that will allow the image to be shown.

We often think of computer forensics as spying or discovery in criminal cases but there are other cases that warrant a closer review of our computer systems — cell phones, personal digital assistants (PDAs) or e-mail systems. If you are the manager of a computer network of more than two or three machines you should think about being pro-active about your computer forensics. Also, when management changes occur, even if they are on a positive basis the leadership should take a forensically sound copy of the computer that was used by the departing executive and save it in a safe place.

To be proactive you may want to institute a policy that makes a forensically sound copy of a hard drive after a key person leaves employment. Some groups would set the bar at directors or ministry leaders. A computer forensic copy can be done in 4-8 hours and would cost less than \$600. To have a truly forensically sound copy of the computer system you should hire an expert. Having chain of custody, encrypted files that can be proven to match the original, ability to search for keywords, and allowing for testimony in court are all advantages to using an expert.

### Track information

Many organizations don't want to wait until someone leaves so a policy is set that they will install a piece of software that tracks everything that goes onto the computer for 30 days. These programs are sometimes called tracers, key logging programs, or tracking programs.

One example of this type of program is called Spector Pro ([www.spectorpro.com](http://www.spectorpro.com)). Spector Pro is a combination of keyboard, instant message, and e-mail logging, along with a screen shot capture. The screen shots let you see a person's session in 10 second increments. If the screen hasn't changed in those 10 seconds, then the snapshot will automatically be deleted. This saves tons of space at night when the computer may be on, but is not active. Many parents use this type of software to track what their kids are doing and saying online.

For networks with more than 50 employees, it may not be

reasonable to review all of the Spector Pro files. For these systems there are document management systems that will help track the usage of your system.

An example of document management is Worldox. This program allows organizations to track all of the documents, spreadsheets, e-mails and other files. It gives an easy user interface for advanced searches based upon keywords, authors, creation dates, or person who last accessed a piece of data. There are logs of who viewed, printed, opened, or changed a file and you can put restrictions on who can delete. In most cases a delete request would be made to the office manager, so that no individual would have that ability.

### Monitor everything

For the mega-networks, those with more than 100 users, there are some great firewall/logging programs. These are expensive (some more than \$250,000), but for a huge corporate network it may be needed. The idea is to have a program monitor everything that goes through the Internet. The program searches for IDs, keywords and unusual file sizes going in and out of the network. Many times it will be "fooled" by people listening to music or watching videos on the Internet. This system also allows customized blocking of Web sites and content.

Some organizations may want to control content coming into their network in the first place. There are many different firewalls to choose from. Most libraries are required to filter out objectionable sites so that they can not get into the system. Others want to scan the content of the information coming in and out of the network.

These devices allow for tracking of who and how much information each user (or I.P. address) is using. If you are going to put one of these systems in place, I recommend that you require individual user names and passwords. Then no matter what computer people use, their Internet username and password will track where they go.

Security is a big expense for equipment, installation, and most of all review. Make sure you plan to put in the time, or allow for your staff to put in the time required to do a good job of reviewing and implementing a tracking or firewall prevention system.



**Jim Harmening is founder of OnTrial Technology, a computer forensics and electronic discovery consulting firm in Orland Park, IL.**  
[[www.ontrialtechnology.com](http://www.ontrialtechnology.com)]



### A COLUMBARIUM *Enhances* BOTH CHURCH & MINISTRY

This new ministry will fulfill the age-old obligation of the church to serve its members from baptism to death, greatly improving Stewardship by satisfying their true needs: a *final Homecoming* to the church.

With twenty-one years experience, Homecoming's caring and professional staff will assist through every phase of project development, from concept to completion. We blend our expertise with a genuine compassion for our client's needs to offer the finest columbarium available, and meet the memorial needs of church members... now and for generations to come.

*Please contact us for more information about our products and services and to arrange a presentation at your church.*



**HOMECOMING, INC.**  
Columbarium Systems, Products & Services

P.O. Box 4850 • Scottsdale, Arizona 85261  
(800) 866-8343 • [www.homecominginc.com](http://www.homecominginc.com)

**Accufax**

**We know where to look.**  
Thorough, confidential, honest & reliable Background Screenings

Protection for your most treasured assets . your children . your finances . your business . your reputation.  
Accufax's 20+ years of experience, provides reliable background screenings for every area of your life.

800.256.8898 [Accufax-us.com](http://Accufax-us.com)