Government Searches of Computers

Reprinted with permission from the August, 2010, edition of the Business Crimes Bulletin, © 2010 ALM media Properties, LLC. All rights reserved. Further duplication without permission is prohibited.

By William A. Whitledge and Justin A. Thornton

You get a frantic call from in-house counsel for your corporate client: "IRS agents with search warrants are seizing our computers as we speak," she informs you. Your mind races to identify the issues that inevitably will arise so that you can promptly, properly, and professionally advise your client what to do. Your client has no experience with criminal investigations and no inkling what will happen over the next few months. She urgently wants to know:

What's going on, what are they going to do?

- Will we get our computers back?
- How long will it take?
- Are they going to find anything?
- What do we do next?
- How much will it cost?

This article addresses some of the issues arising from searches and seizures of computers and their data to provide guidance so that counsel can effectively represent the interests of their clients who are subjected to such intrusive evidence gathering by federal law enforcement authorities.

'What's Going On? What Next?'

The activity at the client's premises is the start of a structured process performed by highly skilled, trained agents who specialize in forensically preserving and extracting evidence from computers. You and your client will usually not have contact with the computer forensics examiners, as they do not have investigative responsibility for the case.

The first step in that process is to preserve and capture the digital data by making a forensically sound "image" of the client's storage media (hard drives), using tools that verify the accuracy of the image and duplicate everything on the seized computer. The image will show the agents not only everything that the user knows is on the computer, but also information the user thought she had deleted and other information, generated by the operation of the computer, of which the user is unaware.

Several vendors make specialized software to read the image files. How far and how deep an examiner will go into a particular image depends on the nature and importance of the case and the needs of the case investigator. The examination in a financial fraud case will focus on the user files and e-mail messages. Cases revolving around Internet usage may require the examiner to reconstruct the user's Internet browsing history and find the sites she visited during a particular time period. Other cases may require the investigator to spend significant time analyzing trace evidence, artifacts, and the computer-generated data to determine, for example, what devices were connected to the computer, when files may have been deleted, etc. At the end of that process, the investigating agent will receive the files of interest and a report of the forensic examination. That report should be provided to you in discovery.

When Will We Get Our Computers Back?

It will probably be some time before your client sees its computers again. Processing backlogs of many months are common, and the law allows the government to retain computers until it has copied and verified the images. Unless the computers contain contraband or are subject to forfeiture, your client is entitled to their return after the imaging is completed.

The immediate goal, however, is to restore normal business operations without the missing computers. You and the client should assess the impact of the seizure and determine whether any of the seized computers contain critical information that is not available elsewhere (*e.g.*, on servers, off-site backup tapes, etc.). You are then ready to contact the lead agent or the Assistant U.S. Attorney and ask him/her to expedite the imaging and return of the critical computers. One solution short of a complete return is to get the government to make you copies of the images, which can then be used to extract the information and transfer it to new computers. If the government refuses your request or is slow to respond, your only recourse is a motion for the return of the property.

ARE THEY GOING TO FIND ANYTHING?

In assessing this question, you should assume that any information that was ever put on one of the seized computers is still there and now in the government's hands. You need to assess how records were kept, when and how records were retired or destroyed, which employees were involved with the issues under investigation, and where other records may be found.

WHAT DO WE DO NEXT?

Deciding how you should proceed requires an evaluation of several factors, not the least of which is cost. One productive starting point is to decide what role the digital evidence will play in the case. If you conclude that very little of the information on the seized computers will be relevant to the investigation, that the government may not be interested in the data, that the client truly knows what is in the seized data, or that the computers may not contain significant defensive data, you may be content to wait until the government provides discovery and shows you what they have found. This is a lower cost strategy that allows you to focus your time and the client’s resources on other data (*i.e.*, e-mail) that you believe will play the most significant role in the investigation.

If, on the other hand, you and the client believe that the seized information will be significant to your defenses, you must devote resources to getting copies of the seized data or reconstructing it. It is important to make the request for copies of the images as soon as possible after the search to try to establish a time line for the return of the computers or a copy of the images. If a large number of computers were taken, focus your request on the ones you believe contain the most important information so that you can have access to it as early as possible (being mindful, of course, of the possibility that your request may alert the government to potentially harmful information it may have missed).

You will also begin to search the rest of the company files for relevant information in the parts of the computer network that the government did not seize. Finding evidence (good or bad) in a computer system requires understanding how the client uses computers and how they are managed. You will need the services of someone, either from the client’s staff or an outside consultant, who can advise you on digital evidence issues and assist in locating and preserving important computer files. This is not normally a task that should be assigned to the company’s IT staff, which usually has no training and expertise in digital evidence issues.

WHAT IS IT GOING TO COST?

The short answer is, “a lot.” Whether you elect to wait for the government’s discovery or actively try to replicate the government’s search, the costs of collecting and analyzing the digital evidence will quickly mount. If you decide to conduct your own search and analysis, you will need expert help from the outset of the case. Even if you wait, you will need that help at the time the government provides discovery. Expert time is expensive, and the work is time consuming for the expert, the lawyers, and the client’s staff.

Data collection and analysis should begin with a plan that includes both legal and technical input. The experts should help determine where to search, what to look for, how to preserve what they find, how to arrange and store it, and how to search and analyze it. The initial plan should also include a process for loading appropriate data into litigation support software and a means to provide online access, or copies of data sets, to everyone on the defense team. If the government has provided copies of the images it made, you and the expert should develop a cost-effective analysis plan that focuses the expert on the information that is important to you.

E-mail may become the most important evidence in any criminal investigation. Unfortunately, it is also one of the most expensive forms of evidence to capture, preserve, and analyze. Many messages appear multiple times within the same mailbox and across multiple mailboxes. The process of locating, “deduplicating,” and reviewing those messages for content, relevance, and privilege is expensive and time consuming. It may be more cost-effective to have an expert do an initial search of mail and attachments for relevancy and privilege using specialized tools and search techniques than to devote attorney time to a review of all the individual messages in a data set.

CONCLUSION

Computer search warrants are becoming more common as more information is stored in computer systems. As soon as a search warrant is executed, it's time to consider what role the seized digital evidence will play in the investigation and how much effort, money, and other resources you need to devote to collecting and analyzing the client’s computer files. The passive approach — doing nothing until the government provides discovery — is an appropriate (and cost effective) response in some situations, but active data collection and analysis may be preferable in other cases. Either way, a well-developed plan of attack that identifies the resources and outside experts you can call on for the technical aspects of the case will make your work with the digital evidence more fruitful and productive.

William A. Whitledge (Tony@Whitledge.org), a former attorney in the Department of Justice's Tax Division and former head of IRS Criminal Investigation Division’s electronic crimes program, provides litigation consulting and computer forensic services to lawyers on issues of information technology and digital evidence analysis. **Justin A. Thornton** (JAT@ThorntonLaw.com), a former federal prosecutor and member of this newsletter's Board of Editors, is a Washington, DC, white-collar criminal defense attorney.