



August 2002 - Special Feature

Collecting Evidence from Providers



Unearthing and preserving digital evidence is a painstaking process by any investigator's standards. But, whether a company is involved in an internal or criminal investigation, staying on the trail of clues can prove even more complicated when the tracks lead to a service provider. We have gathered opinions from experts in the U.K. and U.S. on what corporate executives, investigators

and attorneys should be mindful of as they pursue clues that might be offered up from a provider's electronic cache.

Some Notable Points

by John Weichman

One of the most important things to remember when dealing with digital evidence from an Internet service provider (ISP) is to try to obtain the data as quickly as possible. Most ISPs only keep back-ups for a very short period of time – sometimes only days.

The second most important factor is knowing the appropriate person to contact within an ISP company and realizing that you are likely to need a court order specifying the exact data you want – such as the IP address in question, the name and address of the client, logs showing the usage of the account and copies of emails. Do not be surprised if ISPs seem uncooperative. Their job is to take care of their client's needs, not yours.

Third, know where to serve your subpoena or warrant. Getting the

Finding exactly who to deliver the paperwork to is almost as complicated as obtaining it. You cannot just walk up to, call or fax the nearest office. Most ISPs have procedures in place that must be followed, and if you're not aware of the exact steps to take, you're wasting your time. For example, you may need to contact the ISP's security department. In many instances, local law enforcement officials can point you in the right direction.

Lastly, don't expect to deliver the court order and walk away with the information you need. The reality is that it may be several days or even several weeks before you receive the information you need. Delays can result from the logistics involved in getting to the supervisor in charge of the servers or the back-ups that you are requesting. Additionally, the ISP may need time to duplicate information.

The most important thing to remember is to start the Internet data acquisition process as soon as possible. If not, by the time you complete the required tasks, the data you need may no longer be available.

John Wiechman is CEO and president of TLSI, Inc., a data recovery and computer forensic firm based near Dallas, Texas. He can be reached at (800) 465-TLSI or at john@tlsi.net.