INTRODUCTION TO COMPUTER FORENSICS

BY LYNN ROTH

In the last few years, the use of computer forensics has become more and more common in litigation. This typically involves an "imaged" or duplicated data source (i.e., computer, flash drive, etc.) used to provide a snapshot of data as it existed at a particular point in time.

What Exactly is Computer Forensics?

Computer forensics is the analysis and preservation of electronic data to ensure that electronic evidence is not lost. This critical evidence includes the underlying substantive data and associated data, such as data trails and time/date stamps. These data trails and other markers are often the key to establishing a timeline and co-relating important events. Appropriate computer forensics techniques are also helpful in establishing a chain of custody.

A forensics expert can be used in a variety of ways: as an expert witness, for litigation support, to conduct Non-Invasive Data Acquisition (NIDA), to proactively investigate potential disputes before they end up in court, to recover data negligently or intentionally destroyed, and more.

If You Suspect You Need Forensics Help:

1.) **Step 1: Identification**
   a. Identify the suspect/employee and which devices they had access to, including laptops, PCs, servers, thumb/jump drives, etc.
   b. If possible, remove all devices and secure them, starting a chain of custody including information such as user's name, location of the device, date/time of removal, who removed the device and where the device is stored. (By doing this, you are getting the best possible evidence and making sure that the evidence isn't compromised.)

2.) **Step 2: Preservation** – Contact a computer forensics expert to image the devices. In imaging, the device is hooked up to a writeblocker and a bit-by-bit image is created (exact copy of the drive). It's then verified to ensure that nothing has changed on the original drive.

3.) **Step 3: Extraction/Analysis** – A computer forensics expert can assist you in determining the parameters of your matter (i.e., the key issues, people, key words, date range, etc.).

4.) **Step 4: Presentation/Reporting** – A computer forensics expert can provide you or your client with a report of findings and may be able to testify in court.

What Types of Devices Contain Data?

Computers are the most obvious data sources – but they are not the only ones. Typical data sources include:

- PC
- Laptop
- Server
- Thumb/jump drive
- CD/DVD
- Cell phone/PDA
- Floppy disk
- Tape media
- External hard drive

What Types of Data Are Potentially Relevant?

Although e-mails and Microsoft Word documents are the most obvious types of data you might want to review, there are numerous types that might be critical evidence in any given case:

- E-mail
- Web mail (Hotmail, Yahoo, AOL, etc)
- Plain text and documents
- Images
- Calendar files
- Contact files
- Databases
- Spreadsheets
- Digital faxes
- Audio files
- Video files
- Websites
- Computer applications
- Viruses and spyware

Common Questions and Answers

When is the best time to contact a computer forensics expert?
As soon as possible – preservation is the key.

How do I remove a computer that is turned on?
Pull the power cord from the back of the computer; do not shut it down normally. This will preserve the volatile data that would be lost once the computer is shut down and/or rebooted. Volatile data can include important information such as what documents were printed, clipboard contents and data in memory. The information may be critical to the evidence.

CONTINUED ON PAGE 14 ▶

INTRODUCTION TO COMPUTER FORENSICS

CONTINUED FROM PAGE 13

Can I just have an image taken of a device?

Yes. This is referred to as "preservation only." Once the device is imaged, you are free to redeploy the machine back into the working environment.

Can't my IT person or another employee look through the data?

Absolutely ***not***; every time the drive is turned on and accessed, data is being changed, deleted and/or overwritten. Another question worth asking is "Do I feel comfortable putting that person on the witness stand instead of a forensic specialist?"

What industries does computer forensics deal with?

Some of the main industries include legal, healthcare, government, transportation, high-tech and pharmaceutical, but it's potentially relevant to any dispute likely to end up in court, including business disputes, divorces, insurance claims, etc.

An employee departs the company and a few weeks later the company notices a drastic drop in sales and/or clients. Can forensics help in answering the obvious question?

Forensic specialists can acquire and analyze the hard drive for evidence of communications with the departed client about moving to the new company. They can also determine if files, such as client lists, were copied to removable media and/or e-mailed through a corporate or web-based (personal) e-mail.

An employee was fired for lack of production; now he/she is saying that he/she was wrongfully terminated. Can the proactive use of forensics help?

Yes. A forensics specialist can determine Internet history artifacts including deleted Internet history files and search for non-work-related activity and provide a detailed report to the client.

An employee leaves the company and starts working for a competitor. In a short amount of time, the competitor releases a new formula that your company was working on for months/years.

Forensic specialists can determine if the employee "stole" the formula, whether it be via a thumb drive, external hard drive, or e-mail to a third party or webmail account. NL

LYNN ROTH is director of forensics at ADR Computer Forensics. Roth is based in Cincinnati, but has worked for law firms all over the United States, assisting with large and complex antitrust cases. Roth can be reached by phone at (513) 588-2771 or by e-mail at lynn.roth@adrdata.com.

E-Discovery vs. Computer Forensics – E-discovery and computer forensics are *not* co-extensive. Whereas e-discovery is typically sufficient, forensics offers more detail and should be viewed as complementing e-discovery in many cases. A brief comparison:

E-DISCOVERY	COMPUTER FORENSICS
Collects only active files	Acquires the entire device including deleted files
Returns an abundance of files to the client	Analysis of the data is performed by forensic specialists using parameters given by the client
Reviewers manually go through each document and determine if it is relevant to the case	The client will get a detailed report of the findings from a forensics specialist
Need to hire an expert witness or have IT staff testify	Offers expert witness support
High overall cost	Costs less than e-discovery