

## Article

### Track Former Employee's Computer Activities

*(The following is a theoretical scenario staged to help the reader understand the essential role that a computer forensic expert plays in tracing the theft of intellectual property.)*

An employee (Jane Doe) preparing to leave ACME for a competitor, NEWCO, wanted to make sure that she could take all of her clients with her to her new place of employment. Ms. Doe thought it would be important to have the customer database, marketing plans and product blueprints from ACME so that when she pitched new proposals at her new job, she would be able to win the deal against ACME by placing NEWCO's price offering just under the price likely to be offered by ACME.

On the week before she left, Ms. Doe began collecting data from numerous sources and saved this information to a removable hard drive she had recently purchased. A few weeks after Ms. Doe left ACME, a long time client called the president of ACME to let him know that Ms. Doe had sent an unsolicited proposal to his company and that Ms. Doe was extolling the benefits of her widgets at NEWCO versus those offered by her former employer.

ACME's management had never thought that Ms. Doe was the type of individual who would do this sort of thing. ACME consulted their lawyers who informed them that they needed to act quickly in order to preserve the confidentiality of the documents taken by Ms. Doe.

ACME decided to hire a computer forensics firm to conduct an examination of Ms. Doe's work laptop, owned by ACME. Fortunately, the computer had not been used since Ms. Doe's departure.

The first step taken was to forensically image the computer used by Jane Doe. Imaging involves making a bitstream copy of a hard drive. It ensures that the computer forensic expert can look at the exact match of the suspect hard drive without having to alter original evidence.

At the end of the imaging process, the copy was authenticated as being a genuine copy of the original by generating a hash value, which is a digital fingerprint meant to uniquely identify a set of data, distinguishing it from other sets of data. This value can be generated for an entire set of data (e.g. the whole universe of data on a hard drive), or an individual file (e.g. a Word document). It is an industry-standard means

of authenticating evidence. Should any activity be performed on a computer, whether it be deleting a file or something as simple as changing a single character in a document (e.g. altering a comma into a colon), the hash value generated would be different.

Therefore, if a copy of the original has been made, both should have an identical hash value. To maintain a proper chain-of-custody, the computer forensic expert imaged the original media, documented and validated that the hash value of the original and the copy were the same and kept the original media (suspect drive) sealed while he used the copy (evidence drive) for evidence analysis.

During analysis of the evidence drive, the forensic examiner was able to uncover 20,000 files, including a series of confidential PDF files that had been deleted from Ms. Doe's computer the day before her departure. These documents were originally on ACME's network in a secure storage area that only the IT manager and VP of Sales had access to.

ACME had many questions to which they wanted answers:

- Who accessed these PDF documents at our company besides the IT manager and VP of Sales?
- What did Ms. Doe do with these documents?
- Has Ms. Doe been using these PDF documents on her new computer at NEWCO?
- Did anyone else at NEWCO know of Ms. Doe's actions?
- Did they encourage Ms. Doe to share our information with her new employer?
- Do any of our files or intellectual property exist or did they ever exist on our competitor's computers?
- What else did Ms. Doe do before she left our company?
- Did Ms. Doe begin working for NEWCO while she was on our payroll?

To answer these questions, ACME turned to the computer forensics firm, who advised them that they needed the help of the judge to order production of NEWCO's computers for a forensic examination. NEWCO's attorneys objected with the following arguments:

- Our information is confidential.
- The cost involved in producing our computers is too great.
- This will cause immense disruption to our business and will be too burdensome.
- The scope of the search is too broad and isn't focused... seems like a fishing expedition...

ACME overcame these objections by following the computer forensic expert's recommendations below:

- Agree to forensic-imaging by a third party selected by the defendants
  - Reduces disruptions
  - Reduces cost for requesting party and all parties involved
  - Doesn't compromise evidence when using an expert trained in the field of computer forensics
- Perform search of entire hard drive using agreed upon keywords that are focused and likely to generate relevant documents
- Generate hash values of ACME's intellectual property and then compare these hash values against those of all files imaged on NEWCO's computers to see if there's a match
- Agree to allow the responding party to review the hits found by the expert prior to being produced to ACME's attorneys
- Agree to have all parties bound by a protective order
- Consider filtering files by time frame
- Remove known files from the production set (Operating System Files, Application Files, etc...)

These suggestions, when performed a step at a time, were all it took to move forward with getting access to NEWCO's computers. A stage-by-stage approach often yields better results than asking for everything at once.