Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.

For additional articles like this one or to watch my one hour CLE seminar video go to:
http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

How Not to Investigate a Suspected Data Theft

There are few reported cases that reflect the problems that can result from computer investigations being inexpertly performed. *U.S. v. Koo*, 2011 WL 777965 (D. Or. March 1, 2011), decided this month by an Oregon federal district court, illustrates what can go wrong when a novice directs a computer investigation.

The underlying facts of the case are not atypical. Lawrence Hoffman, the owner of a manufacturer and distributor of after-market auto parts known as the Hoffman Group, discovered on eBay that JES Suppliers, LLC was offering to sell one of his products. A corporate records check revealed that JES Suppliers had been incorporated by a former Hoffman employee and two current employees, including Shegbao Wu who worked for a Hoffman Group subsidiary in China where he managed the design and manufacture of products. *Id*. at * 1.

As part of his investigation, Hoffman asked Wu to return from China to company headquarters in the U.S. under the pretext of discussing company business. While Wu was at the company office, Hoffman asked Wu to leave his company-owned laptop computer in order to replace it with an upgraded computer. The individual who took possession of Wu's computer was an outside computer analyst hired to examine Wu's computer. In examining the computer, "the computer analyst opened a folder named "private" [in Wu's laptop containing documents allegedly relating to JES Suppliers, LLC] and moved it to the laptop desktop" from which he "copied selected parts of the "private" folder onto a USB external hard drive device using" regular business software that was not one of the standard forensic softwares. *Id.* at *2.

Thereafter, "Hoffman took the laptop home and, over the course of two days, periodically booted it up and looked around." *Id.* Hoffman later "testified he "could have" moved files, but did not delete files and did not run the defragmentation utility" and "made "screen shots" of a chat program contact list, which he saved to a subfolder in the "private" folder he named 'QQ.'" *Id.*

Hoffman provided both the laptop and the software backup of the private file to the FBI. As a result, Wu and the other two incorporators of JES Suppliers were indicted for various federal crimes including conspiracy, wire fraud, theft of trade secrets and computer fraud. As part of their pretrial motions, the defendants moved to exclude the back up of the personal file and the

laptop from evidence to be offered by the government at their criminal trial. The court held a pre-trial evidentiary hearing on the motion.

The defendants attacked the software backup of the private files copied from Wu's computer on two grounds. First, they claimed "that computer data can be changed or deleted, and a savvy computer user can cover up such work." *Id*. at *5. From that premise the defendants asserted that the computer analyst "and Hoffman could have uploaded incriminating information onto Wu's computer, altered the dates associated with that information's uploading, installed . . . [the business software] to overwrite the data associated with that change, and then made a selective digital image of the hard drive to turn over to the FBI." *Id.* The court found no evidence to support the defendants' position and held that "[t]he mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility." *Id*.

Second, the defendants attacked the software backup of the private file on the ground that the software used to make the backup was not a forensic software and thus "failed to capture all of the data on the laptop." *Id*. The defendants correctly argued that the business software backup was not "a bit-for-bit copy known as a 'forensic image'" and did not contain the hash values of the files, known as digital fingerprints, and did not capture the computer's unallocated space where deleted files reside. *Id*. at *6. The court, however, found that the government met its burden under Fed.R.Evd. 901 of showing authenticity and relevancy, but also held that the lack of completeness of the evidence relates to the government's burden of proof and is a point which the defense was free to argue to the jury.

While admitting the evidence of the software backup of the personal file, the court took a totally contrary view on the admissibility of the Wu laptop. The court granted the defendants' motion to exclude the laptop because the government could not "make a prima facie showing that the Laptop image was in 'substantially the same condition' as the laptop seized from Wu." *Id.* at *7. The court relied on the hearing evidence not only showing Hoffman's personal animus against Wu because he had filed a civil lawsuit against Wu but found "[m]ost importantly" that "the evidence adduced at the hearing supports the notion that Hoffman tampered with the laptop, which resulted in the FBI imaging 'bad stuff.'" *Id.* at *8.

The court relied on the hearing evidence that "Hoffman himself admitted to booting the computer up and perusing its content over the course of two days" and the defendants' expert who testified "from his forensic examination of the two Images, between the time the . . . [software backup] was made and the time the FBI took possession of the laptop, over 1,000 files or folders were accessed, altered, or deleted" and his findings of "285 files on the . . . [software backup] Image that were absent from the Laptop Image." *Id.*

This case provides two clear lessons to any company that suspects one of its employees of stealing data. First, as a general rule it is usually not a good idea for someone in the organization, particularly a small organization, to conduct the investigation into the suspected theft when the employer could be accused of bias against the employee. The court found that

Hoffman was biased because he had filed a civil action against Wu and the other defendants "the day before he obtained Wu's laptop." Id. at *7. Any issues of bias could have been eliminated if the investigation had been conducted at the direction of outside counsel with expertise in computers and criminal investigations. Hoffman should never have been directing the computer analyst or personally reviewing the computer.

Second, it is critical to hire a qualified computer forensic examiner to conduct the computer examination. What is striking about this case is that the computer examiner hired by Hoffman neither used forensic software to copy the private file nor did he image the entire computer. Instead, he used business software that was not capable of capturing the complete file, never mind the entire computer to preserve it in the exact condition when it was retrieved from Wu. Instead, Hoffman kept the laptop, reviewed it himself, thereby leaving himself open to charges of manipulating, deleting and changing the laptop data.

Indeed, without attributing any bad motive to Hoffman, his opening of Wu's computer would have necessarily and unwittingly destroyed files and time date stamps that could have provided valuable evidence. There is more to computer investigations than simply hiring an investigator. What is critical is that the investigation be coordinated by an attorney with an expertise in computer crime to ensure that the necessary computer evidence is gathered and preserved, that proper procedures are followed including the use of state of the art forensic techniques and software and that a chain of custody on the computer evidence is preserved to rebut any claims that the computer evidence is not in the same condition as when it was initially retrieved in the investigation.