



**THIS ARTICLE  
PROVIDED  
AS A  
COURTESY  
OF**

**JANUS ASSOCIATES, INC.**

**Forensic seizure -  
a case study**

*By Patricia A.P. Fisher*

**JANUS Associates, Inc.  
9 West Broad Street, 9<sup>th</sup> Floor  
Stamford, CT 06902  
203-251-0200**

**[www.janusassociates.com](http://www.janusassociates.com)**

## **A JANUS Associates Case Study**

### **FORENSIC SEIZURE**

#### **Introduction**

This case study is one of a series dealing with specific issues within the computer forensics practice at JANUS Associates, Inc. Their purpose is to discuss experiences in conducting various unique forensic engagements within our specialty areas, computer hardware and software, and to improve specialists' abilities to conduct accurate, supportive computer forensics engagements.

This particular engagement required JANUS to: (1) act as an agent of the Court in the seizure of data; and (2), recreate the seized information including all information that was deleted and/or erased. Time was of the essence because the plaintiff believed the information might be deleted and/or destroyed. Therefore, defendant notification was not provided since, if the defendant was, in fact, guilty, counsel believed that s/he would be predisposed to irrevocably destroy the information, including the facility in which it was located.

An order was served in a civil proceeding within two days, which was as quickly as all parties could assemble. The order was intended to focus on inspecting defendants computer system, restoring any data deleted from the system to the extent that was still possible, and copying all data still residing in the system. A particular problem was that information regarding the specific kind of computers that were in use was unavailable. Since we were unable to determine what hardware was installed, we were also unable able to ascertain what software was resident on the computers (that would be copied and ultimately restored), how old the equipment was, if a network was involved and if so, what other computers were connected to it.

In dealing with hardware, the forensics specialist must utilize proper equipment from his/her case of hardware, since we were asked to make an assumption that the hardware would be of an IBM compatible type, we brought with us a supply of computer components that would mirror IBM compatible equipment.

The software problem was of a greater concern than what hardware was being utilized. With literally thousands of programs available on the market, computer forensics professionals cannot

possibly be an expert in all software products and additionally, all versions of these products. In this situation, we were requested to assume that they were, again, IBM compatible. While this is often a good guess, obviously, there are situations where this might not be the case.

No one could venture a guess about what software was installed. This is particularly important to understand prior to commencing an engagement since it can directly affect how the data capture operation is undertaken. There are various methods for capturing every bit on a computer storage device and in memory. Some are very conservative and others aggressive. JANUS always chooses to be conservative with other people's information since a serious mistake here could seriously result in damage – to information as well as equipment. Computer clocks can be pulled and allowed to run down to work around well-designed passwords structured to prevent initial sign-ons. Hard drives can be pulled out of a machine to thwart program passwords and installed in another computer for copying. However, these practices should only be undertaken when more conservative methods will not suffice.

## **The Process**

To carry out this assignment our first activity was to meet the U.S. Marshals who were serving the seizure order near the intended location in as unobtrusive a manner as possible. The JANUS staff was told the location but no meeting place was preset. Thus, in order to not draw attention to ourselves, we did not appear at the intended location until the appointed hour. This could have become a problem if one of the parties encountered an obstacle to getting to the location – none of the others might have known. We suggest setting up a meeting point for all participants in this type of operation.

Upon entering the site, we requested that the U.S. Marshals, as they secured each floor of the location, also ensure that people were moved away from all computer systems, thereby preventing the equipment from being tampered with, in order to allow us to begin the seizure process.

Our first step was to inspect the premises to determine what type of computers were installed. There was a network in place. This was immediately disconnected to prevent changes to data from outside the site (as well as inside) and ensure that the data within the network server remained as it was when we entered. Upon completion of this inspection we noted each computer, with an assigned number, within a drawing of its location within the facility. Once the census was complete, we began an inspection of each individual computer, numbering and labeling each associated component to match the computer system and building schematic.

The three JANUS staff divided their duties so that they could operate as efficiently as possible. One person began unloading the equipment we were bringing into the site for the engineering

processes that were about to begin. A second person devoted his time to labeling, disconnecting, reconnecting, and rebooting equipment. The team leader focused on the defendant staff, the plaintiff's representatives (who were videotaping the process), and the two lawyers.

Beginning in a conservative mode, the team connected a JANUS computer to a defendant's and began to copy data. However, this proved to be difficult since the office environment itself was extremely dirty and the equipment was placed in a way that precluded our computers from being attached. Thus, each computer was labeled, prepared, and then moved into a temporary laboratory set up in an available conference room as it was needed.

Structuring a seizure assignment to use a temporary laboratory (instead of working at each employee desk) can also be beneficial for the defendant. It allows the forensics equipment to be more efficient since it does not need to be unhooked, moved, and re-established. The result is that the forensics team can move more quickly through the site, preparing, copying, re-cabling and rebooting completed machines for the defendant while another machine is being processed. In the case in question, within a short period of time some staff were able to commence their work.

The second JANUS staff member carefully labeled each connection and their corresponding entry ports, into the computer so that it could be accurately disconnected and reconstructed in the temporary laboratory. This was an important step since much of this particular equipment was old. Old computers very often will not work properly with newer components, eliminating any opportunity to efficiently mix and match. In completing a forensics process care must be taken to ensure that all components work together, especially the peripheral components; e.g., keyboard, cables. Even attaching some other plug than the original type can introduce an error into the process.

It was necessary that the Team Leader, working with on-site management and the legal representatives, spend a considerable amount of time answering questions about the process being conducted so that the technical staff could continue their work. In addition to assisting the defendant through the process, she managed the entire procedure so that:

- Each party's needs were acted upon as well as possible. Each of four groups, U.S. Marshals, plaintiff legal counsel, defendant legal counsel, and defendant had a number of technical questions about how the process would work (and their role in it), how we could accommodate each, and how we could make the entire operation more efficient for everyone.
- Priorities could be established for the computers so that we could uncouple, copy, reinstall

each and enable the defendant to get staff back to work. The defendant made several prioritization requests during the day and these were honored as well as possible, and

- The process remained as efficient as possible from a technical perspective. This is an important consideration in such an undertaking. Conducting a bit-by-bit copy is a time consuming, detailed undertaking. Efficiency is critical so that the process can be concluded within any sort of reasonable time.

The senior technical consultant, who worked exclusively in the temporary laboratory, specialized in the copying process. He connected each defendant computer to the JANUS equipment, enabling the special forensics bit-by-bit copying process to be started. As in many forensics operations, he encountered numerous computers containing passwords. The defendants made several of these available but indicated that they did not know others. When this happens it is imperative that research be commenced immediately to find someone (either defendant or their computer consultant) who knows the password (only as a last resort should the hard drive be removed or the password process physically circumvented). This engagement required several methods. Discussions with the plaintiff revealed several passwords. However, in the case of the network server, none was forthcoming. A discussion with the consultant who installed the hardware and the software revealed a set of passwords, none of which worked. Eventually, the password had to be physically circumvented on this machine. This considerably slowed down the entire process.

An additional problem became apparent near the close of the business day. The defendant's attorney interpreted the seizure order as requiring only copying, not removal of the computers to a JANUS laboratory. Since this operation was on a Friday, he requested that we return on Monday. The JANUS forensics team decided that we could not leave until the entire process was complete since we were unable to secure the equipment and data to our satisfaction at the defendant's site – believing it impossible for us to verify that the data would be exactly as we had left it or that the data would even exist upon our return. This necessitated a call to the court and a request for an amended court order allowing removal of equipment, software, and data to the JANUS lab. After some negotiation, this permission was granted and the amended court order faxed to the seizure location.

Several computers and software were packed in padding, loaded into the JANUS vehicle, and transported to the company laboratory where they were secured prior to the team's retiring for the night. The next workday, the copying process continued from the JANUS location. A partial shipment of computers was returned within two days and the last computer, shortly thereafter.

## Summary

There are several steps a legal team can take to ensure the simplest process for itself, the least obtrusive for the defendant (to minimize any recourse possible on the plaintiff client), and the clearest direction for its computer forensics partner (to maximize speed and minimize cost). First, any seizure order should be carefully structured with early input from the computer consultant so that its scope encompasses all the potential activities involved with copying, as well as possible physical removal if needed.

The computer consulting forensics manager should be included very early in discussions regarding the goal of any seizure. This will assist him/her to help structure an appropriate seizure order *from a technical perspective*. What was once clear and concise in a legal sense, is now difficult to comprehend in a world of computers where one CD can contain an entire encyclopedia's worth of information.

The forensics consultant also needs to have time to think through the appropriate computer wording of any seizure order so that it meets all the goals of the legal team. A telephone conversation where an intended seizure order is read, without time for thoughtful input, can be detrimental to the overall legal case. A case could depend on something that may appear to have no relevance to the data in question such as whether to seize voice mail.

Fourth, whenever possible the forensics expert needs to understand what type of hardware/software is in use in the location. This may be the most difficult of all. Legal counsel may not be able to determine this with any certainty. However, by discussing what plaintiff counsel is looking for (the type of data), the forensics team can narrow the possible software platforms down to typically a few from the hundreds or thousands available.

In the case in question, old copies of software were installed on the primary target computer. Interpretation (by defense counsel) of the seizure order that the court accepted did not allow removal from the premises of the documentation for this old software. Much discussion went back and forth between counsels, the computer consultant, and the Court over what software could be removed. This resulted in a slowing of the recreation process while JANUS acquired the specific version of the installed software so that this last portion of the seizure order, that of recreating and inspecting the defendants' computer system, making every effort to restore or salvage any data deleted at any time, and then copying all data, including all restored or salvaged data, could be completed and presented to the Court. Although the software could be acquired for this particular case, it is even more important to understand that old software may not be able to be purchased. Therefore, a seizure order should specify that the software *and its documentation* be seized.

Fifth, it is important to determine the size of the target environment. This will dictate how much equipment is brought to the site and how many staff are needed. The computer forensics task is a slow, painstaking operation and it is important to size the environment properly so that appropriate numbers of staff may be assigned. Without the correct numbers of both equipment and people, the forensics process may not be able to be completed within a window, which the Court finds acceptable. If that happens, data critical to the case could be lost. In this particular case, defendant's staff cooperated with the JANUS team. This resulted in a smoother operation and a more rapid return to operation for them. However, if a defendant opposed the procedure, did not produce passwords, etc. having an adequate number of staff could become critical.

It is also important to define the specific operational environment into which the computer forensics team will enter. As is the norm, in this case the court order specifically named the JANUS staff that was to participate in this operation. Thus, people with predetermined, specific skills were reserved. Encountering a much larger environment upon arrival could put the entire process at risk. Potentially, even more serious problem could have occurred if the JANUS team had encountered a different technologic environment. Macintosh technicians usually are not as skilled when working with IBM - PCs. The same is true of the opposite. Such a miscue could result in people with the wrong skills being named in the court order and included on the team, with the result being errors or a slowdown while appropriate staff was rounded up. Because the computer world is so diverse, this is an important consideration. In this particular case, plaintiff counsel could not define numbers of computers, type of computers, where they all were (which legal jurisdiction), etc. If the network server had not been on the premises, but rather in the other state where more than one computer on the network did reside, valuable evidence might have been lost. Although a well-educated guess will be done (and worked in this case) this might not always be so, particularly where heavily customized software is installed.

Computer forensics can play a major role in assisting legal counsel to successfully undertake the discovery process in a computerized environment. However, the success of this is, in large part, dependent on a need for the legal community and the computer experts to work closely together through the entire process, not only at the moment that the computer searching takes place. The computer forensics person understands the very specific world of computers. The lawyer deals with the very ambiguous world of law. These are two very different worlds and work best when both combine their expertise to produce needed results.

FSACS032006