

Computer Forensic Evidence Preservation

By: Mike Dwyer - Senior Litigation Solutions Consultant

As computer forensics continues to play a bigger and bigger role in civil litigation matters, it is important to note that certain actions, as well as certain non-actions, can affect the integrity and admissibility of digital evidence. To ensure that your digital evidence is preserved, Project Leadership has developed the following "What to Do" and "What NOT to Do" guidelines to assist you in your digital forensic matter.

What to Do

- ✓ Contact a reputable Computer Forensic company to perform the forensic imaging and/or conduct the investigation. Ask for references.
Verify ownership of the suspect computer(s). Does your client have the legal right to have the suspect computer(s) examined?
- ✓ Begin a proper Chain of Custody for each individual piece of suspect media (computers, hard drives, USB thumb drives, CD/DVDs, etc).
- ✓ Record any and all dates, times, names, and locations that you would consider appropriate for your case.
- ✓ Record Make, Model, & Serial Number (or Service Tag) information of suspect computer(s).
- ✓ Record the method of how the suspect computer(s) was/were powered down.
- ✓ If possible, take possession of the entire suspect computer(s), not just the hard drive(s). Additional information can be obtained from the physical computer, including BIOS date & time information and the boot up order of the computer. This can be very important if date & time information is critical to your case.

What Not to Do

- ✓ Do not turn on the computer, even to just to "take a look around". Hundreds of changes take place when a computer is turned on, including changes to many files date and timestamp metadata.
- ✓ Never have a member of the IT department collect data or conduct an investigation. They are not trained in forensic processes, procedures, and methodology. Their actions could comprise the integrity of the data and render it inadmissible.
- ✓ Never log into the suspect computer as the suspect custodian(s). This action makes it very difficult, and sometimes impossible, to tie data and/or actions to a suspect.
- ✓ Do not leave the computer(s) connected to the company network or internet. The computer(s) should be stored in a secured location until it is handed over to a reputable forensic company for forensic imaging and analysis.
- ✓ Do not allow the computer(s) to be continued to be used by a custodian. This could result in many vital artifacts being intentionally or unintentionally destroyed and unrecoverable.

Michael Dwyer is a Senior Litigation Solutions consultant for Project Leadership Associates. Mike is an experienced Litigation Support manager, with deep operational and technology experience, a technology consultant, and Litigation Support consultant and provides on site consulting services for law firms and in-house corporate legal staff for international, national and regional law firms.