Following the Proper Chain of Custody for Electronic Discovery

Legal professionals are beginning to prosper from the benefits of electronic discovery as electronic documents are being increasingly utilized to assist them in winning cases. It has become clear that the discovery process associated with electronic documents is no different than the process followed for more traditional discovery and that the only change are the tools and storage media used. Electronic discovery is allowing for faster, more competent, and more effective review of documents, as the process of sifting through enormous quantities of paper becomes increasingly rare.

As a proper chain of custody is crucial to the collection of electronic evidence, the following two elements should be employed to ensure that such evidence would be found admissible in a court of law:

Principle

A chain of custody is necessary to show that the integrity of the evidence has not been compromised during its production, as it details the precise manner in which data was collected, evaluated, and preserved. The following must be included in a chain of custody log: a list of all media that was secured, the precise information that has been copied, transferred, and collected, and proof that the information has not been changed.

Procedures

All electronic evidence collected must be properly documented each time the evidence is viewed, and such documentation must be made available throughout the discovery process. The following forms of documentation should be recorded in the chain of custody log:

Initial Data Collection

- Name of investigator who took possession of the electronic evidence
- Precise date, time, and place from which the collection was made
- Name of the individual turning the electronic evidence over
- Specific explanation of the evidence gathered, including:
- Type of media, standard and manufacturer
- Serial numbers and/or volume names
- Type of information
- Description of information

- Any writing on labels on the media
- Status of any write-protection on the media

Specific Data Collection Procedures Followed

- Specific tools used throughout the collection process
- Name of investigator performing each procedure
- What occurred from each procedure
- Any problems encountered throughout the collection process

Additional Documentation

- Precise information regarding the transfer of evidence
- Precise information regarding the purpose of any transfers
- All date and time information regarding when media was removed from storage
- Information regarding a visual inspection of the media
- Explanation of data analysis performed, including:
- Specific tools used throughout the analysis
- Name of investigator performing analysis
- What occurred each time the analysis was performed
- Any problems encountered
- Any other information deemed important to the investigation

Conclusion

By following the above chain of custody procedures, the electronic evidence collected throughout the investigation will be found admissible by a court of law. The fragile and volatile nature of electronic information requires orchestrated efforts to ensure electronic evidence is protected and maintained to facilitate its thorough analysis by a computer forensic specialist and its introduction into an active litigation. A critical aspect of this is the execution of clearly defined and well-documented chain of custody procedures.