Chain of Custody

Maintaining the Chain of Custody in Civil Litigation

MERRILL LEGAL SOLUTIONS

Contents

Introduction	1
Stages of electronic discovery	1
Chain of custody - forensic acquisition	2
Chain of custody – non-forensic acquisition	4
Chain of custody log	6
Outsourcing chain of custody management	8
Final thoughts	9

Introduction

Chain of custody is a familiar concept in criminal law, but until recent years it was foreign to civil litigators. In the criminal law arena, police would seize evidence, seal it in a plastic bag, label it, and sign it in to a locked evidence room. If the evidence was taken out by anyone for any purpose (for example, for laboratory examination or testing) that withdrawal would be noted on the log, as would its return. The next removal from the room would likely not be until its presentation at the trial itself.

Historically, evidentiary chain of custody was rarely an issue in civil litigation. With the advent of the digital age, it has become a major issue because the actual nature of evidence in civil litigation has undergone a radical transformation — from tangible paper to electronic data.

Electronic discovery is a multi-stage process, and custody is an issue at every one of those stages

In the seminal electronic discovery publication,[1] regarding the importance of chain of custody, the author states:

> The purpose of testimony concerning chain of custody is to prove that evidence has not been altered or changed from the time it was collected through production in court. *Gallego v. United States of America*, 276 F.2d 914 (9th Cir. 1960) (citing *United States v. S.B. Panicky & Co.*, 136 F.2d 413, 415 (2d Cir. 1943)). Chain of custody testimony would include documentation on how the data was gathered, transported, analyzed, and preserved for production. This information is important to assist in the authentication of electronic data since it can be easily altered if proper precautions are not taken.

It's also much more complicated to handle electronic data as evidence than it is to sign in tangible narcotics confiscated at the time of arrest and sign them out again at the time of trial. That's because electronic discovery is a multi-stage process, and custody is an issue at every one of those stages.

Stages of Electronic Discovery[2]

The generally accepted stages of electronic discovery are identification, preservation, collection, processing, review, analysis, production and, finally, presentation as evidence during trial. The requirement to maintain the chain of custody applies to all stages of the electronic discovery process. Because the discovery process has so many steps, the chain of custody can be very long and convoluted.

The Amended Federal Rules require the preservation and disclosure of "electronically stored information" (ESI). The admissibility of ESI will hinge, in part, on laying a proper foundation for the electronic evidence.

Often, the chain of custody for digital information involves documenting the methodology used in the forensic acquisition of ESI contained on storage media, such as a hard drive, and the chain of custody of the ESI during and after the retrieval process. The foundation for admissibility of ESI may be attacked by objecting to either prong of the process.

[1] Michael R. Arkfeld, Arkfeld on Electronic Discovery and Evidence, § 8.10(C), *Chain of Custody*.
[2] Electronic Discovery is also referred to as discovery of Electronically Stored Information [ESI].

Chain of Custody - Forensic Acquisition

Much of what has been written on chain of custody shows how rooted the concept is in its history as a criminal evidence requirement. A law enforcement tone continues to permeate the practice. In fact, many computer forensic investigators working in the civil litigation arena come from law enforcement backgrounds, and for seizing and making a forensically exact image of a hard drive in a hostile situation, no one is better suited. Say, for example, that a court orders the seizure and inspection of a husband's personal laptop in a contested divorce proceeding. The forensic investigators, acting for the wife's attorney, arrive at the door of the husband's residence with the court order[3], seize the physical laptop, attach copying equipment to it, and make a bit-by-bit image of the entire hard drive.

A forensic investigator might photograph a laptop, record its make and model number, its serial number, the date it was seized and the "hash" value or "electronic finger-print" of the entire hard drive.

This is not just copying files, this is copying *everything* on the hard drive: slack space and deleted files that have not yet been overwritten, for instance those deleted e-mails to and from a paramour, deleted brokerage accounts and banking records, Internet surfing history, the works. They use tools such as Guidance Software's Encase[4] or Forensic Tool Kit[5]. These devices are designed so that the act of copying the data — an activity that normally would change some information or metadata on the source hard drive — alters nothing on the source hard drive. The ribbon through which stored data passes is a one-way street, outbound only.

The chain of custody documentation required to this point is fairly straight forward. The seizing personnel first take a photograph of the laptop, record its make and model number, its serial number, the date it was seized, and very importantly, the "hash" value or "electronic fingerprint" of the entire hard drive. The next step is the forensic copying of electronically stored information or ESI to a pristine hard drive. After completion of copying the data to a pristine hard drive a hash value is taken of the drive to which the data was copied. The hash value of the new drive, if the process was performed properly, will match the hash value of the original drive.

[3] In Canada, Australia and the UK, such orders can be obtained *ex parte*; they are called "Anton Piller" orders, from the English Court of Appeal decision first authorizing this procedure, *Anton Piller KG* v. *Manufacturing Processes Ltd.*, [1976] Ch. 55. In the US, a "civil subpoena" may be issued, but it is done within the context of an already-commenced litigation.

[4] See http://www.guidancesoftware.com/

[5] See: http://www.accessdata.com/common/pagedetail.aspx?PageCode=ftk2test

What is a hash value? A hash value is an electronic fingerprint. *"A hash value can be applied to a file, a section of a disk, or a whole disk, and recorded. The hash value will change if the data in a file, section or disk is changed or altered."*[6]

One type commonly heard of is the MD-5 Hash Value. Here is an example of what it looks like, generated from a commonplace phrase:

("The quick brown fox jumps over the lazy dog")
= 9e107d9d372bb6826bd81d3542a419d6

Even a small change in the message will result in a completely different hash. For example, changing d to e:

("The quick brown fox jumps over the lazy **e**og")
= ffd93f16876049265fbaef4da268dd0e

Another hash value algorithm is called SHA-1. Instead of 32 characters, it has 40. Here is what it looks like on the same phrase:

("The quick brown fox jumps over the lazy dog")
= 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12

As with the MD-5, even a small change in the message will result in a completely different hash. For example, changing dog to cog:

("The quick brown fox jumps over the lazy **c**og")
= de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3[7]

The hash value change resulting from the alteration of merely one single character in this sentence results in a change as dramatic as if "War and Peace" had been edited to become "The Cat in the Hat."

The "chain of custody" rule requires that admitted exhibits "be preceded by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The original laptop can then be returned to the husband. The original electronic content of the laptop, now stored in its new pristine location, is the evidence of interest. It is this copy which must now be retained properly to establish authenticity. All further logging of custody will be done with respect to the exact duplicate ESI on the new hard drive — the forensic copy. Best practices demand that at this point a working copy be made of the forensic copy and that the first forensic copy be locked away or secured in such a fashion as to avoid any alteration, damage or spoliation. All further chain of custody logging will now document access or changes to the working copy — when it was taken to the lab, what files were reviewed, etc.

In this scenario, the tangible and the intangible — the hard drive and the data thereon — are almost one and the same. In these situations the courts will accept the ESI stored in its original source as virtually indistinguishable from the ESI stored on the new source (the forensic copy with an identical hash value). The court will therefore accept the foundation for the forensic copy and approve its admissibility. This type of forensic acquisition has been effectively employed for years and has resulted in a forensically defensible chain of custody.

[6] Michael R. Arkfeld, *Arkfeld on Electronic Discovery and Evidence*, § 5.5 (B), at page 5-40.
[7] These examples of hash values were obtained from Wikipedia: http://en.wikipedia.org/wiki/MD5 and http://en.wikipedia.org/wiki/SHA_hash_functions.

Chain of Custody – Non-Forensic Acquisition

Many articles written about chain of custody in civil electronic discovery presume that the initial data extraction is always done in this forensically exact manner. In fact, it is not. Forensic ESI collection is primarily utilized when there are early issues regarding suspicion of fraud, theft of intellectual property, concealment of assets, or other indicia of concealment including deliberate spoliation of ESI.

In the clear majority of civil litigation such forensic collection of information is not anticipated. Instead, civil litigation requires preservation, review and production of information relevant to the matters at issue in the litigation, as established in Fed. R. Civ. P. 26(b)(1) which reads:

> Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition and location of any books, documents [defined elsewhere in the rules to include "electronically stored information" (ESI)], or other tangible things.

Most of the time, the only thing that's potentially relevant is the *active data* on the computers and network file servers and in the e-mail boxes of the people and departments of a company that have anything to do with the subject matter of the litigation.

This is the basic scope of civil discovery rule; nothing here about kicking down any doors or seizing anything.

However, identification and preservation of relevant electronic evidence is only part of the issue. It remains key during the collection of this evidence that the chain of custody be kept intact to ensure its admissibility in court. As one author noted[8]:

> Depending on the circumstances of the case, a chain of custody foundation will assist in the admission of evidence. When there is a chance of confusion, or that data may have been altered or tampered with, evidence establishing a chain of custody is important. …The "chain of custody" rule is a variation of the requirement under FED. R. EVID. 901(a) that evidence must be properly authenticated or identified prior to being admitted. *United States v. Turpin*, 65 F.3d 1207, 1213 (4th Cir. 1995) (citations omitted). The "chain of custody" rule requires that admitted exhibits "be preceded by evidence sufficient to support a finding that the matter in question is what its proponent claims."

In the majority of cases, nobody is interested in what may have been deleted from a computer hard drive, or what the user's Internet surfing history might have involved. Most of the time, the only thing that's even potentially relevant in litigation is the *active data* on the computers and network file servers and even more likely in the e-mail boxes of the people, and departments, that are related to the subject matter of the litigation.

We are not usually talking about busting into a hostile location and seizing computers to make forensically exact copies of hard drives. Nor are we talking about making forensically exact copies of the hard drives of our own personnel's computers. While the cost of doing so has come down recently, copying entire hard drives is still much more time-consuming and expensive than making copies of specific folders and files from a target custodian's laptop or network server.

What happens in most civil cases with discoverable electronic data is that the data is collected in a more "informal" manner from the custodians' machines and their mailboxes on the Exchange server and the Outlook PST files on the custodian's machine. This may require that the data collector move around the office from machine to machine and from server to

[8] Michael R. Arkfeld, Arkfeld on Electronic Discovery and Evidence, § 8.10(C), *Chain of Custody*

server, but instead of making a complete forensic copy of every hard drive he touches, the collector is making copies of just those files and folders deemed relevant at that time. The collector may in fact be aggregating those copied files on just one portable hard drive via the USB connector.

While this process is "informal" in comparison to the rigid protocols and specialized equipment used in making forensically identical copies of hard drives, it is a process that still must comply with basic standards of forensic soundness. An electronic fingerprint must be taken to verify that the file which has been copied is identical to the file on the original user's hard drive. This fingerprint, once again, is our "hash value" as described before — applied down to the level of the individual file.

The hash value is the critical element that carries through the entire chain of custody, through every step of the discovery process.

Recently, collection software or appliances have become available which claim to be able to retrieve ESI in a forensically sound manner without all the steps essential in a traditional forensic collection. These software applications, or appliances, begin the collection process by plugging into any location on a computer network. From that location, these tools seek to create a map of all the data on that network, and then collect data from any server, desktop, laptop, or other device on the network, without having to move from one location to another to accomplish the collection. Whether this device is used, or whether the more traditional "place to place" collection is done, it is critical that the hash value of each file or folder that is to be copied be recorded at the time of acquisition, and then matched against the hash value of the copied version to insure accurate duplication and maintain the standards needed for authentication. This step is critical. If the hash marks on the copies do not match, this informal forensic copy (which is also the copy proffered to the court for introduction into evidence) may lack sufficient foundation to be admissible. It is easy to see why this process is problematic and should not generally be attempted by in-house technical staff or by an amateur. The admissibility of the ESI will rely upon the sophistication of the collection methodology and the personnel involved in the collection process.

The hash value is one of the critical elements that carries through the entire chain of custody, through every step of the discovery process. If at some point there is an objection to the chain of custody record, the hash value of the file being offered as evidence in court — if it is identical to the hash value of the file originally collected from the hard drive of person X — will provide one of the necessary foundational elements for admissibility. Aside from the hash value of a file, it is essential to provide a legally defensible chain of custody log explicitly documenting where, when and how the ESI was preserved, collected, and processed.

This is a looming trap for any party attempting to introduce electronically stored information. If the opposing party objects to the ESI, a complete foundation for the ESI will have to be laid. If the collection process was done in-house, there may be no competent witness available to testify regarding foundation who is not also a party to the litigation. The ESI may be excluded as a result. In addition, if the ESI was collected by someone lacking in qualification or experience, or if the collection methodology utilized does not satisfy the court, the ESI may be excluded from evidence. Due to the problematic nature of ESI collection and custody, there is a strong argument for the use of an electronic evidence service provider, or e-discovery vendor, who is also qualified in forensic collection methodology. This guarantees that the collection of ESI will be completed in a forensically defensible manner as well as assuring that should the need for a forensic witness become essential, you are ready.

Chain of Custody Log

Maintaining a proper chain of custody log is an essential element of any defensible collection method and will assist in laying the foundation for the admission of ESI. The chain of custody log for electronic evidence in civil litigation, in the vast majority of the cases where forensic hard drive imaging is not utilized, will, at a minimum, contain the following:

Information from the collection stage. This will include a description of all devices from which data was copied (including model numbers, serial numbers, and locations of each device); a description in each case of which folders were copied; and the process used for making the copies. The collection procedure should create a hash value for each file during the process of reading the file, either by direct copy from the individual machine or over the network. These hash values should be stored, along with a copy of the file in its native format, on the media onto which the data is copied. As part of the collection documentation, a collection "manifest" should be created that includes a list of files collected, their location, and their hash values. This manifest can be used to compare the hash value of the collected file with the hash value of the file produced at the end of the review.

As part of the collection documentation, a collection "manifest" should be created that includes a list of the files collected, their location, and their hash values.

Although anyone can collect electronic evidence and "hash" the corresponding computer files, it may be prudent to have a third-party perform the collection process and generate the hash algorithms. If an objection based on foundation is made regarding ESI, the person responsible for the collection of the ESI may be called to testify at trial to the methodology used during the collection, as well as the authenticity of the evidence. It becomes problematic if the actual client, one of the client's employees, or the client's counsel, is the person who collects the data, as that person may later be required to establish his or her credibility and lack of bias in the collection process.

Shipping to the electronic discovery processing service provider. Many data collection services prefer to personally deliver the media containing the collected data directly to the processing company. In the real world, commercial realities may dictate that a courier be used. While less than optimal, the tracking capabilities of FedEx and UPS both provide the documentation that comports with what's required to maintain proper chain of custody.

As you can see, one of the "best practices" to employ would be the retention of an electronic evidence service provider who can perform all of these functions within the same company to ensure the integrity of the electronic evidence and maintain its chain of custody in a reliable manner

Receipt by the electronic discovery processing service provider. The chain of custody log used by the electronic discovery processing company should, according to the Electronic Discovery Reference Model (EDRM), contain the following:

- Electronic discovery identification and inventory number (a barcode labeling system is recommended)
- Date received
- Matter name
- Client name
- Client/matter number
- Name of person/company/shipper delivering the evidence
- Description of item(s) (including manufacturer name, model number and unique identifier/serial number whenever possible)

- MD5 Hash of each piece of media where possible (electronic fingerprint)
- Name of person receiving evidence (Logged by)
- Check Out (check box—Yes/No)
  - If "Yes"
    - Date
    - Reason
    - Custodian name
  - Name of recipient (used when evidence shipped from electronic discovery provider to another entity)
  - Name of shipper
  - Shipper's tracking number
  - Date of shipment
  - Date of receipt
- Check-in date

At no time should media containing original or copies of client data be left out in an open, unsecured area unaccompanied by the person who is authorized to possess and work with those items.

Whenever the original evidence is accessed, it should only be made available to the small team in charge of logging and securing the evidence. It is clearly preferable to use the copy of the original evidence rather than the original evidence to avoid any damage or spoliation. Any activities involving the original evidence must be logged. After the logging, the owner of the evidence should be sent confirmation that evidence was received.[9]

Processing. The physical premises of the electronic discovery processing company should be designed in such a way that media containing collected data are safeguarded in a secure location to which only a select group of people have access. If media are removed from that secured room, for example to load the data onto the processing servers, the media should be signed out, copied to the processing servers as quickly as possible, and then returned to the locked room with no delay. At no time should media containing original or copies of client data be left out in an open, unsecured area unaccompanied by the person who is authorized to possess and work with those items of media. This is the case even if the entire company's premises are restricted access.

Review of evidence. After "native file" processing is complete, the data should once again be checked against the original copies' hash values to verify that the hash values are still identical. If the processing involves using TIFF (Tagged Image File Format) images, the data is obviously changed and will then yield an entirely different hash value.

At this point, the processed data will either be sent elsewhere — to the law firm for loading on its own internal review system, or to a third party Web host — or, it will be loaded on the e-discovery processing vendor's own Web-hosting application. If the processed data is leaving the e-discovery processing vendor's custody and control, again, proper chain-of-custody logs, related both to the media onto which the data was copied and the form of delivery, should be maintained. Sometimes these deliveries do not take the form of physical media, but rather the form of electronic transmission — files attached to e-mails, or sent via FTP (file transfer protocol). The chain-of-custody baton is now passed to that recipient, the law firm, or third-party Web host.

If the processed data stays with the e-discovery vendor for hosting, that vendor's own internal documentation of chain-of-custody logs should reflect the handover from the processing department to the Web hosting department.

[9] http://edrm.net/wiki/index.php/Processing_-_Audit_and_Chain_of_Custody

Confirmation and production of chain integrity. After the review is complete and the reviewing party has chosen what electronic documents to produce to the opposing side, it's time to regenerate the hash algorithms to verify that what's being produced is identical to what was first collected. Conversely, this is the stage where you will be receiving production inbound from the other side. It is essential that you regenerate hash-value algorithms on this incoming data as well before touching it in any other way. This is a crucial anticipatory action in preparation for the next stage.

Presentation at trial. If you find a smoking gun in your opponent's productions and want to present your "smoking gun" at trial, by having made a hash fingerprint of it the moment it arrived, you can prove it is exactly the same as the file you received. Conversely, if one of your own documents is critical to the proof of your case, you may need to refer back to the hash fingerprint of the document first generated back at early collection, to prove during presentation at trial that it is still the same document.

When there is a chance of confusion or that "electronically stored evidence" may have been altered or tampered with, evidence establishing a chain of custody is important.

Outsourcing Chain of Custody Management

Chain of custody is now as important to civil litigators as it is to criminal attorneys. Depending on the circumstances of the case, a chain of custody foundation may have to be rigorously established for the admission of ESI evidence. When there is a chance for confusion, or the risk that ESI may have been altered or tampered with, evidence establishing a chain of custody is crucial. The first step necessary to establish a consistent chain is generally to ask the custodian or a witness about the origin, storage and handling of the electronic evidence. When faced with a case involving a computer record and ESI evidence, this questioning will also involve the procedures utilized to gather the data as well as a determination of how it was copied and preserved. In addition, it will include testimony about the storage media used to store and transfer the data, as well as how the ESI was processed and searched.

The necessity of ensuring the chain of custody for civil cases has risen in importance and must be carefully planned during the acquisition of your electronic evidence. Consideration should be given to having a single third-party service provider collect and process the evidence to ensure standardized procedures are followed. Then, if the collection procedure is challenged, a witness from the electronic evidence service provider can offer relevant testimony, setting forth the chain of custody for the electronic evidence and ensuring that all the links in the chain of custody are intact.

Final Thoughts

The transition of evidence from paper to an electronic format imposes new requirements upon civil litigants to ensure that a proper “chain of custody” is maintained. For years, the forensic collection of ESI in the criminal arena has been well documented and certain standards maintained. With the recent increased emphasis upon the collection of ESI in the civil litigation arena, it is becoming as important to properly maintain and document a "chain of custody" in the acquisition, processing and admission of ESI. From the initial collection of evidence through to its eventual introduction in the courtroom, a properly documented and maintained chain of custody will assist in the admission of electronic evidence. Laying a proper chain of custody foundation will establish under FED. R. EVID. 901(a) that evidence was properly authenticated or identified prior to being admitted. With a properly established “chain of custody” you can be sure that the evidence will be given its proper weight and consideration by the jury.

Now that civil litigants must be equally cognizant of the necessity of maintaining a proper "chain of custody" to ensure the admissibility of ESI, one must make a critical decision regarding who will be charged with responsibility for the data collection and preservation as well as what methodology will be used. Clearly, these decisions should be made in an informed fashion and should contemplate the potential need for an electronic evidence service provider.

About Merrill Corporation

Founded in 1968 and headquartered in St. Paul, Minnesota, Merrill Corporation (www.merrillcorp.com) is a leading provider of outsourcing solutions for complex business communication and information management. Merrill's services include document and data management, litigation support, branded communication programs, fulfillment, imaging and printing. Merrill targets markets including the legal, financial services, insurance and real estate industries. With more than 6,300 people in over 70 domestic and 15 international locations, Merrill empowers the communications of the world's leading companies.

About Merrill Legal Solutions

Clients worldwide rely on Merrill Legal Solutions to provide integrated solutions to accurately, cost-effectively, reliably and consistently manage the complex litigation life cycle. Merrill Legal Solutions combines e-discovery expertise and proven solutions with flawless project management and customer service to impact the outcome of litigation, from small to large high-stakes cases. With a single, end-to-end global provider for your litigation support, discovery, deposition services and trial consulting, you will improve your case management while saving time and money.

Corporate Headquarters
One Merrill Circle
St. Paul, MN 55108
800.688.4400
legalsolutions@merrillcorp.com

www.merrillcorp.com/law