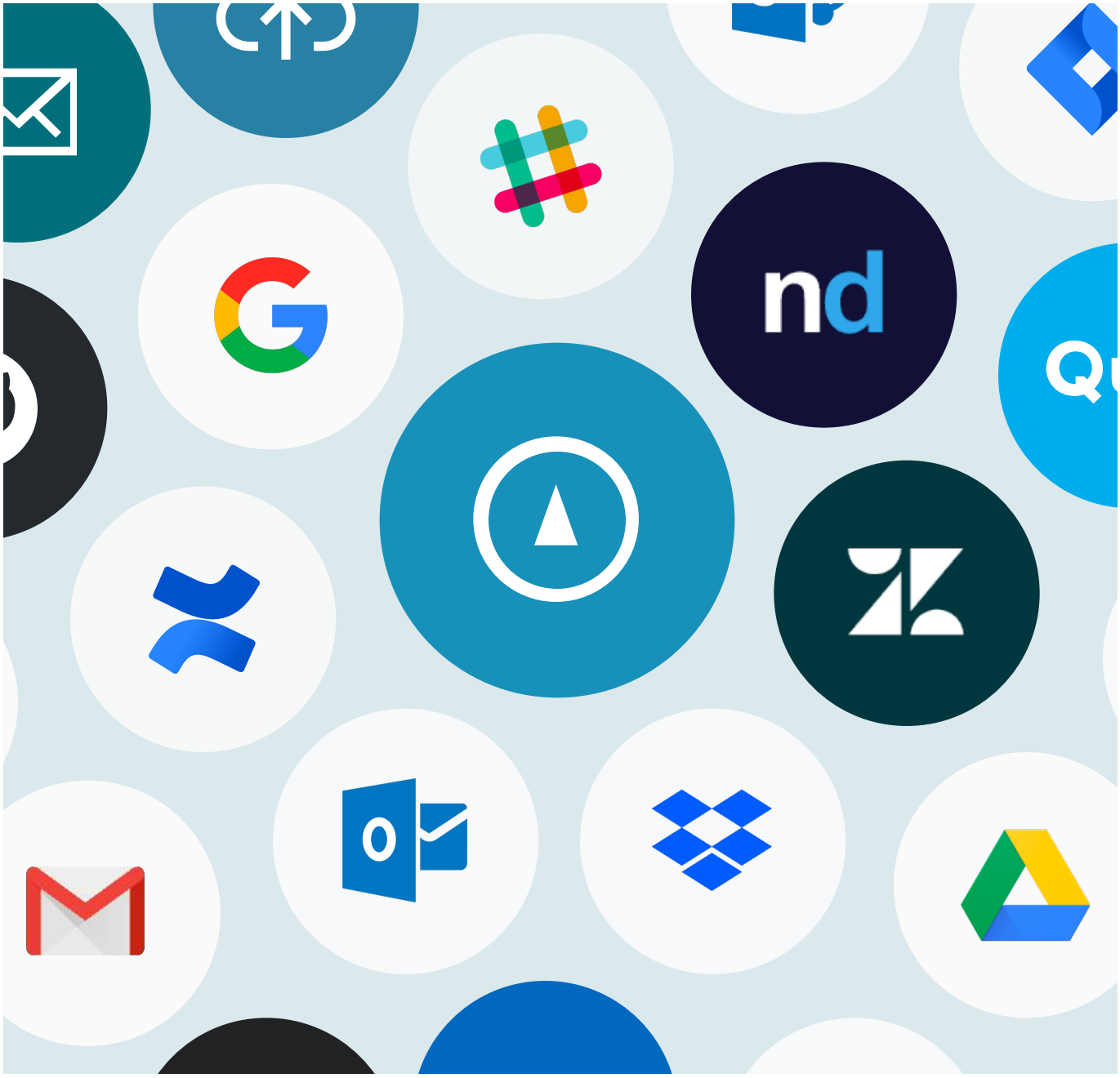
White paper

The Self-Authentication Rules of Evidence for Electronically Stored Information

February 20, 2018



The Self-Authentication Rules of Evidence for Electronically Stored Information

The 2017 Amendments to the Federal Rules of Evidence provide litigants with a new method to self-authenticate electronically stored information (ESI). The traditional trial procedure for authenticating ESI was with a testimonial witness pursuant to Rule 901. The new Amendments provide a method for authenticating evidence without a witness, unless there is an actual challenge to the admissibility of the ESI.

Onna's reporting features can give lawyers the opportunity to use the new self-authentication Rules. A qualified person can perform a collection of ESI to execute a litigation hold. Once the collection is completed, an affidavit can be prepared that documented the steps to collect the ESI with an report containing a list of MD5 hash values of the data. As will be explained below, the combined approach of documentation and reporting from Onna should empower lawyers to have self-authenticating electronically stored information.

Overview of New Self-Authentication Rules

The new Amendments to the Federal Rules of Evidence are Rules 902(13) and 902(14). The Rules state:

> **Certified Records Generated by an Electronic Process or System.**
>
> *A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11)[1] or (12)[2]. The proponent must also meet the notice requirements of Rule 902(11).* [3]

[1] Federal Rules of Evidence 902(11) states: ***Certified Domestic Records of a Regularly Conducted Activity***. The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them.

[2] Federal Rules of Evidence 902(12) pertains to foreign records.

[3] Federal Rules of Evidence 902(13).

Certified Data Copied from an Electronic Device, Storage Medium, or File.

Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).[4]

The Advisory Committee Notes to the new Amendments state the purpose of the Rules are to save parties the expense of calling a foundational witness.[5] Frequently in litigation, authentication is not disputed, thus unnecessarily raising costs with providing a witness at trial.

In order to comply with the new Rules, a litigant must offer a "certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial."[6] This certification can meet the authenticity foundation requirements that a live witness would meet under Rule 901(b)(9) in describing a process that generates an accurate result.[7] In other words, this means a witness who can explain how ESI was collected with forensic software in a defensible manner. Lawyers would typically depose a collection expert seeking answers to the following questions:

What data collection did you perform in this case?
Where did you collect the subject data from, such as a laptop or a smartphone?
How did you collect the text messages from the smartphone?
What data collection device did you use in performing the collection?
What training have you had in using this collection device?
How many data collections have you performed using this collection device?

There many options for additional questions to ask, but the strategy is to have the collection explain they are trained to collect ESI with a specific software,

---

[4] Federal Rules of Evidence 902(14).

[5] Advisory Committee Notes, Federal Rules of Evidence 902

[6] *Id.*

[7] *Id*. Federal Rules of Evidence Rule 901(b)(9) states: ***Evidence About a Process or System***. Evidence describing a process or system and showing that it produces an accurate result.

they used that application to collect data, the application functioned properly, and the process produced an accurate result. As described in a case where reports were generated from computer data, a declarant explained how the information was submitted to the computer system and the specific steps that were done to acquire the results.[8]

The Advisory Committee Notes further explain that hash values can be used to authenticate ESI, because "identical hash values for the original and copy reliably attest to the fact that they are exact duplicates."[9] As such, ESI that has been certified by a person qualified to attest to the fact that hash value of the proffered evidences is identical to the original hash value. [10]

The "qualified person" envisioned in Rule 902 should be someone who can qualify as an expert witness under Federal Rule of Evidence Rule 702. An "expert" is a "witness who is qualified as an expert by knowledge, skill, experience, training, or education." [11] The purpose of this individual is to have someone with specialized knowledge who can assist the trier of fact understand scientific, technical, or other specialized knowledge.[12] Performing enterprise-level data collections arguably would require a "qualified person" to have the knowledge to defensibly collect ESI as an "expert" under Rule 702.

Based upon best practices for authenticating ESI and the plain language of Rules 902(13) and 902(14), attorneys could have experts use the following collection strategies to preserve electronically stored information to likely comply with the self-authentication requirements:

1. A qualified person who understands the collection technology performs the data collection;
2. The qualified person can explain what was done to identify ESI for preservation;
3. That the collection system exported an accurate result; and
4. The MD5 hash values of the copied data are identical to the original ESI.

---

[8] *Friends of Mariposa Creek v. Mariposa Pub. Utils*. Dist., 2016 U.S. Dist. LEXIS 52499, at *35-36 (E.D. Cal. Apr. 19, 2016).

[9] Advisory Committee Notes, Federal Rules of Evidence 902.

[10] *Id.*

[11] *Vitamins Online, Inc. v. Heartwise, Inc.*, 2016 U.S. Dist. LEXIS 16355, at *11-13 (D. Utah Feb. 9, 2016), citing Federal Rule of Evidence 702.

[12] Id.

It is important to remember that the Amendments to Rule 902 do not limit any of the other options for authenticating ESI. The goal in a trial is for evidence to be what it purports to be.

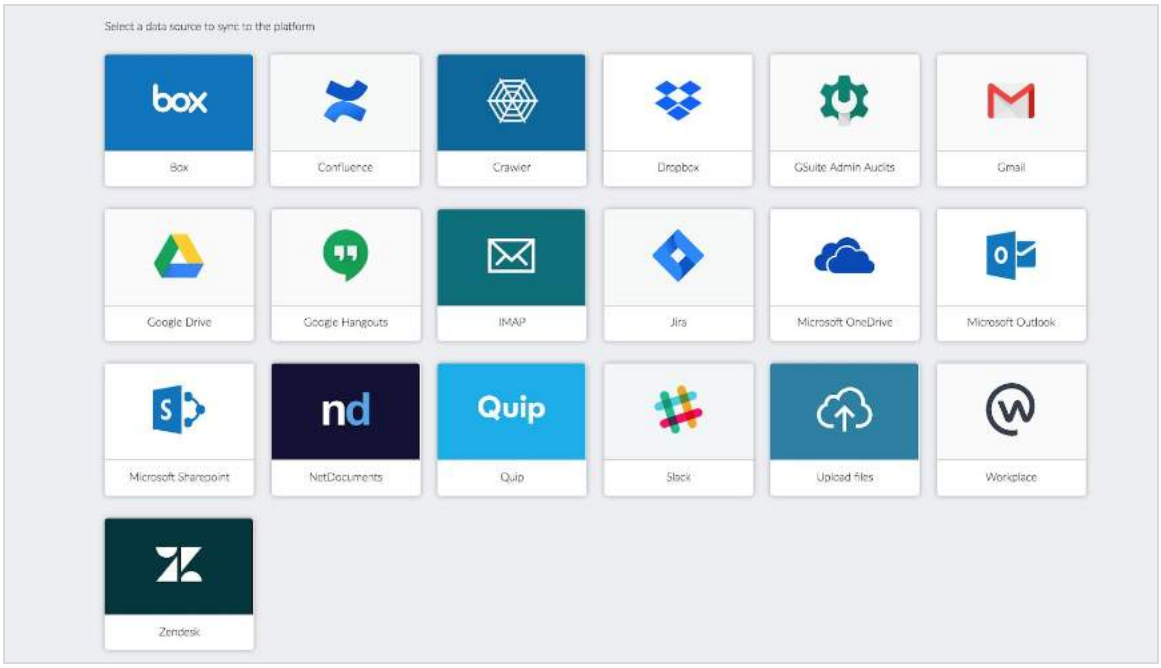
Using Onna with New Federal Rules of Evidence

In order to have ESI that is self-authenticating at trial, attorneys should think about admissibility when they issue a litigation hold. If ESI has been defensibly collected in a forensically sound manner, then a proffering party can make use of Federal Rules of Evidence Rules 902(13) and 902(14). This means how a preservation strategy that can be explained in an affidavit, so a judge can clearly understand what ESI was preserved and how.

Identification of ESI
Onna can preserve ESI on multiple cloud-based accounts across an enterprise using API-based collection. If a data source is collected through a user's account, then the collection process will involve going through an authentication process where the source (e.g. Box) states what Onna is being given permissions to access. Onna then breaks the source down into folders, channels or smaller units from the source to avoid overcollection. The entire account can be collected if necessary.
Sources can also be added with the company credentials. In this case, a company adding GSuite or O365 can select the users from which it wants to collect information.

Preservation of ESI
Sources of ESI can be preserved based on the scope of the case, such as by a specific date range. If there is an ongoing duty to preserve, data sources can be set to continually archive all versions to Onna.
The qualified person preserving ESI can select the relevant sources for collection. Below is a sample workflow for identifying and collecting ESI.

Step 1: Disparate Source Selection

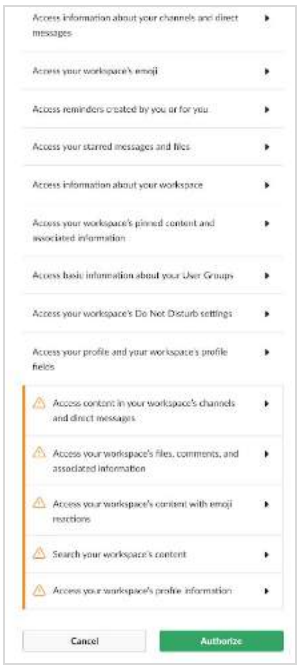


Onna's API-based collection interface.

Attorneys should interview custodians and work with the collection professional to identify the data sources for collection. The goal is to collect what is relevant to the case, without over or under collecting data.

Step 2: Authorization from Source Lists

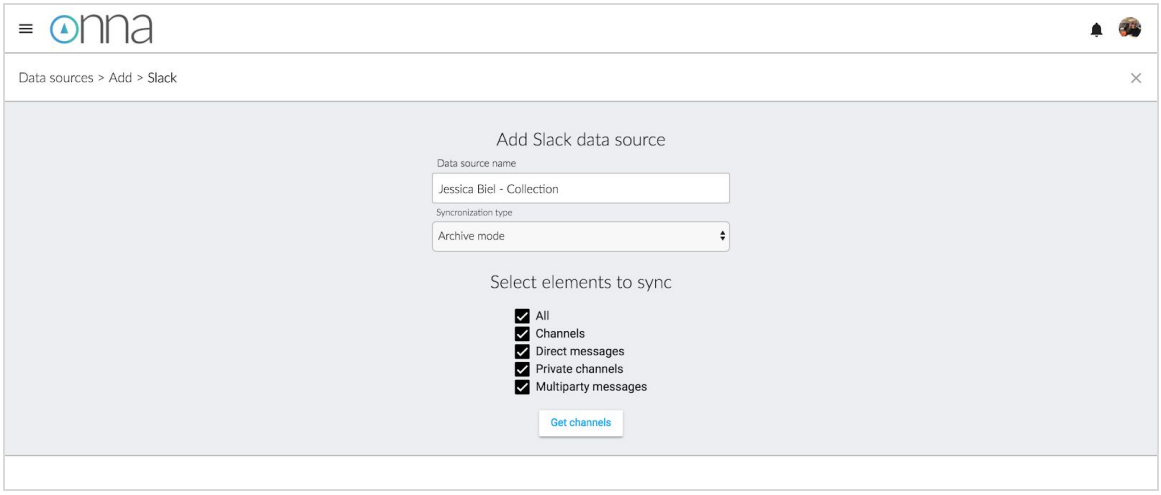
The qualified person collecting the data can select the elements to be collected from the source list. This can be used to confirm the relevant data sources are preserved.



The access Onna can gain through API-based collection

Step 3. Collect Relevant Data

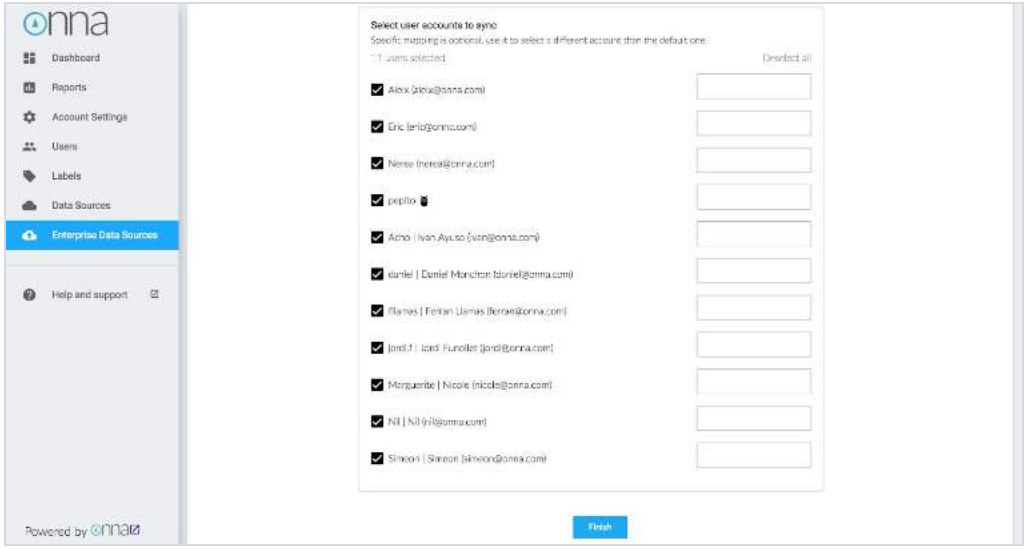
The relevant ESI can be preserved based on isolated data sources or by entire accounts.



After establishing a connection with the API, Onna breaks down the information available from the source. If you know where the responsive data set lies, you can select this fragment of the account

Step 4: Enterprise Preservation

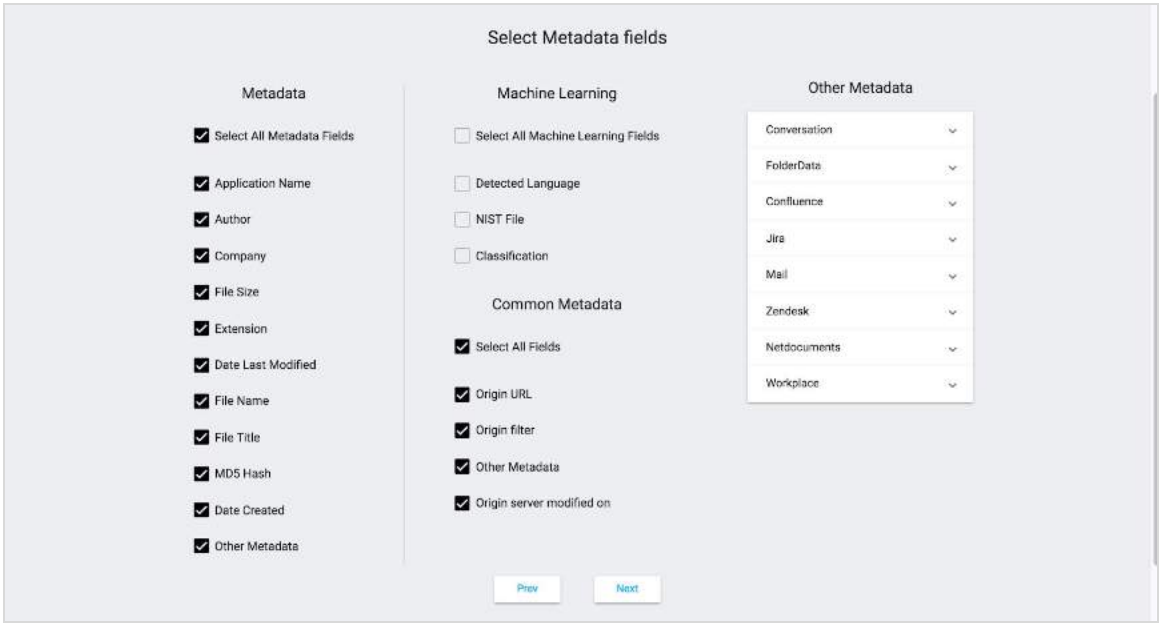
Enterprise wide collections can be executed using the company credentials and allow access to the organization's user accounts without the need for the user credentials



Using enterprise data sources, Onna can access the entire list of users on that source so as to collect information from any user account selected

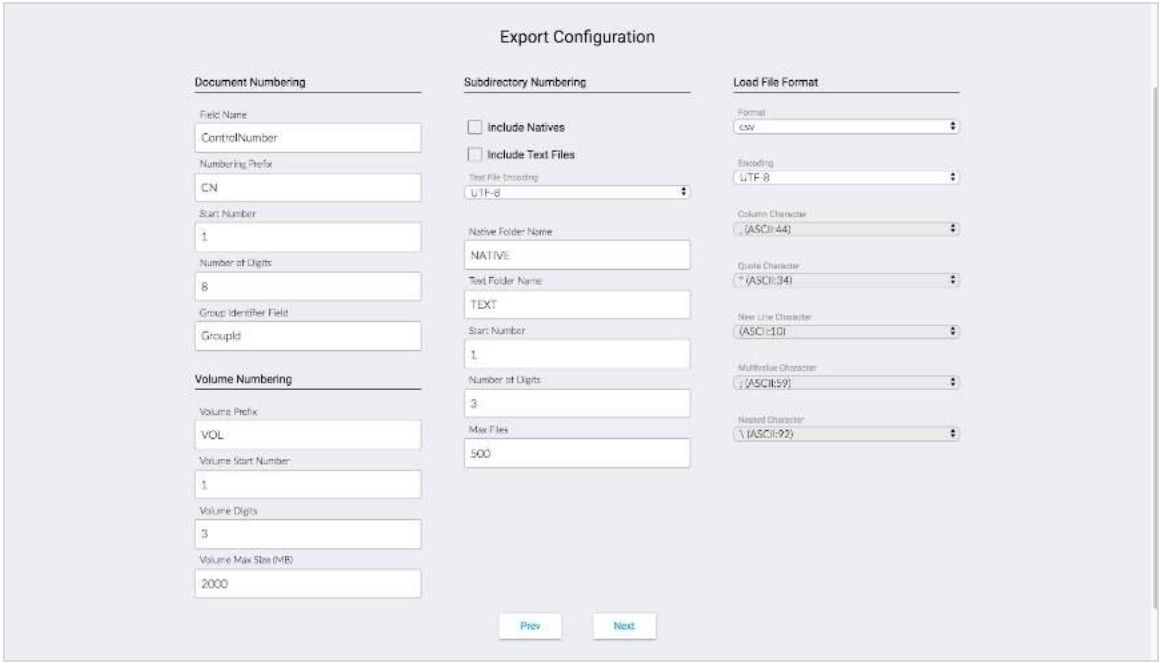
Step 5 Creating a Collection Report

A report can be created with the MD5 Hash value once a collection has been completed.



By collecting directly from the source, Onna has access to all metadata fields available at the origin. It also adds an MD5 Hash value to all documents for identification and reporting purposes

The report is exported as a CSV file with a list of files and any applicable metadata.



Reports can be created as a simple CSV or can also include the natives and text files

Syncing Onna to the Rules of Evidence

Attorneys executing a litigation hold can have a qualified person perform a data collection using Onna. This requires providing a “certification” that has sufficient information to establish that the ESI is authentication, if that person was called to testify at trial. This can be done with a detailed affidavit that documents how the relevant ESI was collected. The affidavit could include how the scope of discovery was determined, what search terms were used to identify sources of ESI, the sources of ESI that were preserved, and perhaps even screenshots. This would help explain both of the technology that was used and what data was collected. A detailed report that includes all collected files, with relevant metadata, and MD5 hash values can be attached as an exhibit to comply with the Rule 902(14).

The challenge for attorneys is the self-authentication Rules of Evidence are still new. It will take an enterprising lawyer to be the first to offer self-authenticating ESI into trial. The question is, who will it be?