WHITE PAPER

Authenticating Digital Evidence Under FRE 902(13) and (14)

Using Digital Signatures (Hash Values) and Metadata to Create Self-Authenticating Digital Evidence

Pagefreezer

CONTENTS

Introduction

Vast quantities of modern evidence is digital and stored in the public and private cloud. Based on societal norms, the growth of digital evidence continues to be exponential. In today's world, authentication of digital evidence is challenging. Just consider some of the digital evidence sources that modern legal matters center around:

Emails

Text messages and instant messages (like WhatsApp)

Social media comments, chat room posts, and forum threads

Conversations and other data on team collaboration tools (Slack, MS Teams, Workplace from Facebook)

Website content and blog posts

Social media posts, photos, and direct conversations

Online video from YouTube, Twitter, Instagram, and Facebook

The problem with this new digital content is that traditional rules around submission of evidence can make it difficult to collect, submit, present, and ultimately defend this new digital evidence in a legal setting.

The Federal Rules of Evidence (FRE), which governs evidence law in United States federal courts and was first adopted in 1975, has struggled to keep up with the rapid evolution of technology, and this has consequently made it hard to understand and comply with requirements around identification, authentication, and admissibility of digital evidence.

Authentication in particular has been a complex issue, since Article IX of the FRE traditionally gave litigators little choice but to rely on a sponsoring witness, such as a forensic technician, to attest to the authenticity of a piece of digital evidence. Needless to say, this is an expensive and time-consuming exercise that slows down the legal process.

Thankfully, this changed with the introduction of Rule 902(13) and 902(14) in December 2017. Under Amendments 902(13) and 902(14), digital evidence can now be self-authenticating, provided it is collected and stored appropriately.

While this promises to streamline the use of digital evidence during legal proceedings, it also requires a new approach to evidence collection. Since FRE 902(13) and 902(14) place an emphasis on collection and authentication, they also invite opposing counsel to question the admitting party's methods.

In an article on the strategic implications of these new rules, Carey S. Busen and Gilbert S. Ketelas of the BakerHostetler law firm argue that:

> *"The new rules will require those involved in collecting and preserving evidence to have protocols that maintain the information the Rules require in the certification. Thus, it will be imperative that organizations, law firms, and vendors employ preservation and collection policies that capture and transfer the required data, including maintaining each piece of data's unique identifier (referred to as a 'hash value'). These amendments do not prevent the parties from stipulating to authenticity, even without a certification. Nevertheless, they may incentivize parties to more aggressively challenge authenticity when it is apparent that an opponent is unable to make the pretrial certification envisioned by the amendments."*

In other words, making use of a collection and preservation method that proves the authenticity of a piece of evidence is crucial—and failing to do so will, now more than ever, encourage opposing counsel to question the authenticity and admissibility of that information.

With the above in mind, this white paper will examine how legal professionals can make use of appropriate tools and services to generate defensible evidence that has hash values (digital signatures) and metadata. By doing this, they can collect and preserve self-authenticating digital evidence that will be accepted under FRE 902(13) and (14).

The Maryland Approach versus The Texas Approach

Any discussion of Article IX of the Federal Rules of Evidence as it relates to digital evidence should start with a brief mention of both the Maryland Approach and the Texas Approach to social media evidence.

In her article, *Authenticity and Admissibility of Social Media Website Printouts*, Wendy Angus-Anderson succinctly discusses the commonly-perceived difference between the Maryland Approach and the Texas Approach to social media evidence. Here is what she writes:

> *The state of the law regarding social media evidence admissibility is murky at best. Courts and academic writings have split the case law into two approaches. These can best be referred to as The Maryland Approach and The Texas Approach.*
>
> *According to analysts, Maryland Approach courts are skeptical of social media evidence, finding the odds too great that someone other than the alleged author of the evidence was the actual creator. The proponent must therefore affirmatively disprove the existence of a different creator in order for the evidence to be admissible.*
>
> *Courts following the Texas Approach are seen as more lenient in determining what amount of evidence a "reasonable juror" would need to be persuaded that the alleged creator did create the evidence. The burden of production then transfers to the objecting party to demonstrate that the evidence was created or manipulated by a third party. This second approach is viewed as "better reasoned" because it allows for proper interplay among the many rules that govern admissibility, including 901.*

Judge Paul W. Grimm (whose seminal 2013 article on social media evidence played a significant role in outlining this distinction) and Kevin Brady summarize the two approaches in the following way in their paper, *Admissibility of Electronic Evidence:*

The Maryland Approach—see *Griffin v. State, 19 A. 3d 415, 423 (Md. 2011)*—demands a higher standard when it comes to authenticating digital evidence. Importantly, there is a high burden of proof on the admitting party to show that the evidence was not falsified or created by another person. To authenticate evidence under the Maryland Approach, the admitting party must provide:

- Testimony from the actual creator of the page or post
- A search of the creator's hard drive, specifically the Internet history and hard drive
- Data obtained directly from the relevant social media site

The Texas Approach—*see Tienda v. State, 358 S. W. 3d 633 (Tex. Crim. App. 2012)*—places a lower bar on the authentication of digital evidence. Here the admitting party merely needs to provide evidence that would satisfy a 'reasonable juror' as to the authenticity of a piece of content. Consequently, the admitting party must provide either:

- Testimony from a witness with personal knowledge regarding the digital content
- Testimony from an expert, or a comparison with authenticated evidence
- Circumstantial evidence

Authentic versus Relevant Evidence (Relevance under FRE Article IV)

It's interesting to note that, while Wendy Angus-Anderson does an excellent job of explaining the differences between the Maryland Approach and the Texas Approach, she actually argues against this distinction and calls it a false one:

> *Courts using the Maryland Approach are not placing an excessively high bar on social media evidence, or even following a stricter standard than the Texas Approach cases. They are simply recognizing that evidence must be relevant before it may be presented to the jury. In the case of website printouts, this means showing that the content reflects a certain webpage and that it was posted by the purported source. Opinions and articles drawing a distinct line between "Maryland" and "Texas" approaches are actually just pointing out the cases in which the second requirement was not fulfilled.*

For their part, Judge Paul W. Grimm and Kevin Brady do not call the distinction false—they argue that it's important for a legal team to know which approach their jurisdiction follows—but they also stress the fact that it is crucial to realize that authentication and relevance remain very separate issues. Even if the admitting party can prove that a piece of digital evidence is authentic, the opposing party can still argue that it's not relevant, or that it's hearsay evidence.

Even if its authenticity has been established, digital evidence still has to comply with Article IV of the Digital Rules of Evidence, specifically, FRE 401, FRE 402, and FRE 403. These rules state the following:

Rule 401 – Test for Relevant Evidence

Evidence is relevant if:

(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and

(b) the fact is of consequence in determining the action.

Rule 402 – General Admissibility of Relevant Evidence

Relevant evidence is admissible unless any of the following provides otherwise:

- *the United States Constitution;*
- *a federal statute;*
- *these rules; or*
- *other rules prescribed by the Supreme Court.*

Irrelevant evidence is not admissible.

Rule 403 – Excluding Relevant Evidence for Prejudice, Confusion, Waste of Time, or Other Reasons

The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.

Article IV and the Limits of FRE 902(13) and 902(14)

It is important to understand that, while FRE 902(13) and 902(14) have in many ways simplified authentication of digital evidence, it has not done away with the requirements of Article IV of the FRE. In fact, since it is arguably now easier to admit digital evidence that a court would deem authentic, issues of relevance will become more pertinent.

As an example, FRE 902(13) and 902(14) might make it easier for an admitting party to submit authenticated copies of an individual's Facebook posts, but as the number of submitted posts increase, opposing counsel is virtually guaranteed to question these posts on grounds of relevance. In simple terms: the easier it is to submit digital evidence, the more evidence is likely to be submitted, and the more opposing counsel will attack its relevance.

To better understand the scope and limits of FRE 902(13) and 902(14), the next section reproduces these amendments in detail.

"In simple terms: the easier it is to submit digital evidence, the more evidence is likely to be submitted, and the more opposing counsel will attack its relevance."

Federal Rules of Evidence: Rule 902(13) and Rule 902(14)

Article IV and the Limits of FRE 902(13) and 902(14)

As mentioned in the introduction, FRE 902(13) and 902(14), allow for the self-authentication of digital evidence, provided it is collected and stored appropriately.

Self-authenticating evidence is nothing new. Prior to December 2017, many forms of evidence were already considered self-authenticating. These included:

- Domestic public documents that are sealed and signed
- Domestic public documents that are not sealed but are signed and certified
- Foreign public documents
- Certified copies of public records
- Official publications
- Newspapers and periodicals
- Trade inscriptions
- Acknowledged documents
- Commercial paper and related documents
- Presumptions under a federal statute
- Certified domestic records of a regularly conducted activity
- Certified foreign records of a regularly conducted activity

New to this list, however, is **Certified Records Generated by an Electronic Process or System (Rule 902(13)):**

Certified Records Generated by an Electronic Process or System

(13) ***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) or (12). The proponent must also meet the notice requirements of Rule 902(11).*

As well as **Certified Data Copied from an Electronic Device, Storage Medium, or File (Rule 902(14)):**

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

(14) ***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).*

In addition to the updated rules, official committee notes related to the amendments were also provided when the new rules came into effect. Although these comments are quite lengthy, they are worth reading before discussing the implications of Rules 902(13) and 902(14), since they provide clarity on the intention behind the amendments.

Comment To 2018 Amendment Adding Subdivision (13)

The amendment sets forth a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Court has determined that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.

The reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this rule to prove the requirements of Rule 803(6). Rule 902(13) is solely limited to authentication and any attempt to satisfy a hearsay exception must be made independently.

In order to provide the adverse party with an opportunity to properly analyze the issue of authenticity, the "record" provided by the proponent of the ESI evidence must include the metadata for the material in question if reasonably necessary to assess the material's authenticity. In addition, a challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

Comment To 2018 Amendment Adding Subdivision (14)

The amendment sets forth a procedure by which parties can authenticate data copied from an electronic device, storage medium, or an electronic file, other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Court has determined that the expense and inconvenience of producing an authenticating witness for this evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure in which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value." A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that the person checked the hash value of the proffered item and that it was identical to the original. The rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology.

"If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates."

> *In order to provide the adverse party with an opportunity to properly analyze the issue of authenticity, the "record" provided by the proponent of the ESI evidence must include the metadata for the material in question if reasonably necessary to assess the material's authenticity. In addition, a challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.*

Comments Regarding Hash Values and Metadata

While FRE 902(13) and 902(14) do away with the need for an expert witness in many cases, the requirements around authentication are still high. Courts demand very convincing proof that any particular piece of evidence is authentic, and as the official comments to both Amendments make clear, **hash values and metadata** are central to creating self-authenticating digital evidence that would be deemed acceptable.

The above comments make it clear that:

- Self-authentication can be achieved by providing a verifiable hash value
- Where possible, the associated metadata of a piece of evidence should be provided

The following two sections of this white paper will examine the real-world implications of FRE 902(13) and 902(14), and discuss how self-authenticating evidence can be created through the use of hash values (digital signature) and metadata.

The Implications of FRE 902 Amendments (13) and (14)

To reiterate what was mentioned in the section on Authentic versus Relevant Evidence, Amendments (13) and (14) do not address issues related to relevance or hearsay—nor can they be used to necessarily prove that a particular individual was the author of a page or post (it could be argued, for instance, that an individual's account was hacked).

In her article, Mining Metadata: The Gold Standard for Authenticating Social Media Evidence in Illinois, author Linda Greene states the following, which acts as a good description of the limitations of Amendments (13) and (14):

> *To illustrate, Rule 902(13) would provide for the authentication of a webpage collected by the Wayback Machine via a certificate attesting to the accuracy of the process used to retrieve it. It would not prove that the defendant was the author of the statement contained therein. Therefore, while these new rules certainly streamline the process of authenticating certain digital evidence, they do not ultimately resolve one of the central issues concerning social media evidence—proving authorship.*

That said, the implications of these amendments are still significant. Consider the typical situation of a case involving multiple copies of webpages and social media posts. As the matter goes to trial, these copies would need to be authenticated. One could roll the dice and not authenticate them, but if opposing counsel questions their authenticity, there's a strong possibility that they will be declared inadmissible. Alternatively, you could try to find a witness to testify to their authenticity, but knowing who exactly would be deemed an acceptable witness isn't always clear, and the whole exercise promises to be expensive for the client and time-consuming for his legal counsel.

So what would be the better choice? Is it better to simply hope that authenticity isn't questioned by opposing counsel, or to try and convince the client that the significant cost of an expert witness would be worth the expense?

Thanks to FRE 902(13) and (14), the cost of expert testimony is no longer necessary. Electronically stored information (ESI), like social media posts and comments, cellphone images, text messages, and website content can, under these amendments, be authenticated without testimony as to foundation. This means that the submission of ESI can be greatly streamlined.

Practical Application of FRE 902(13) and (14)

Gregory N. Heinen of Foley and Lardner explains what this would look like in practical terms:

> *Logistically, these rules would require the proponent of the ESI to present a certification sufficient to establish the authenticity of the evidence, reasonably far in advance of trial, at which point the opposing party would have to determine whether it could actually make a real challenge to the authenticity of the evidence," states Heinen. "This certification would need to be made by a qualified person (someone who would otherwise be able to testify at trial regarding authenticity) and, for the tech-savvy reader, would likely be performed by checking the hash values for the original documents and the copies to ensure they are identical, unless and until future technology provided new methods of identification. If the opposing party did not timely object to the certification, then no authenticating witness would be necessary at trial. The intent of the committee is to encourage parties to litigation to determine in advance of trial whether either intends to challenge the authenticity of any ESI, to appropriately tailor their trial preparation and streamline the trial itself.*

It should not be assumed, however, that legal teams can now pay less attention to authentication of digital evidence. If anything, the fact that ESI can be self-authenticating places an increased focus on authentication methods. Just as opposing counsel is more likely than ever to attack evidence on grounds of relevance, an increase in self-authenticated evidence makes it more likely that an opposing party will question authenticity as a matter of course.

In other words, rolling the dice and hoping that opposing counsel doesn't question authenticity is now a worse strategy than ever. FRE 902(13) and (14) shines a spotlight on ESI that was collected incorrectly.

Gregory Heinen concludes his article with the following:

> *In light of these amendments, it would behoove parties to litigation to make sure, in cases where large quantities of ESI could play a significant role at a potential trial, to collect such ESI using forensically sound methods, including employing specialists in appropriate cases and in any event ensuring that the methods used track the hash values of the documents," writes Heinen. "The clearer the records about what collection practices were utilized, and the more proactive counsel can be about giving notice to the opposing party and obtaining the appropriate certification in advance of trial, the more time and expense will be saved.*

"If anything, the fact that ESI can be self-authenticating places an increased focus on authentication methods."

Self-Authenticating Digital Evidence with Hash Values (Digital Signatures) and Metadata

Understanding Hash Values

The Cybersecurity and Infrastructure Security Agency (CISA) defines a hash value, or hash function, as:

A fixed-length string of numbers and letters generated from a mathematical algorithm and an arbitrarily sized file such as an email, document, picture, or other type of data. This generated string is unique to the file being hashed and is a one-way function—a computed hash cannot be reversed to find other files that may generate the same hash value. Some of the more popular hashing algorithms in use today are Secure Hash Algorithm-1 (SHA-1), the Secure Hashing Algorithm-2 family (SHA-2 and SHA-256), and Message Digest 5 (MD5).

In simple terms, a hash is a specific number string that's created through an algorithm, and that is associated with a particular file. If the file is altered in any way, and you recalculate the value, the resulting hash will be different. In other words, it's impossible to change the file without changing the associated hash value as well. So if you have two copies of a file, and they both have the same hash value, you can be certain that they are identical.

A hash value guarantees authenticity thanks to four particular characteristics:

- **It is deterministic,** meaning that a specific input (or file) will always deliver the same hash value (number string). This means that it is easy to verify the authenticity of a file. If two people independently (and correctly) check the hash value of a file, they will always get the same answer.
- **The odds of "collisions" are low.** This means that the chances of two different inputs (files) coincidentally having the exact same hash value are incredibly small—practically non-existent.
- **A hash can be calculated quickly.** Generating a hash value is quick and easy (provided you have the right tool). The size of the file in question is also irrelevant—generating a hash value for a large file is as simple as creating one for a small file.
- ***Any* change to the input will change the output.** Even the smallest change to the input file will result in a change to the resulting hash value. This means that it is impossible to alter a file without changing the associated hash value, which makes it very easy to prove (or disprove) the authenticity of a piece of digital evidence.

Thanks to these characteristics, **a hash value acts as a digital signature (or fingerprint) that authenticates evidence.** As long as a piece of evidence was correctly collected and processed, the hash value will be exactly the same as that of the original. To see examples of hash values and how they will automatically change based on the inputs, see the section below titled: *Generating a Hash Value.*

Using Metadata to Authenticate Evidence

Alongside hash values, metadata can also be used to prove the authenticity of digital evidence.

Metadata provides information about digital data. In other words, it's the data about data. As an example, the metadata of a social media post would include information about the author of the post, the message type, post date and time, versions, links (un-shortened), location, likes, and comments.

Metadata Types

Metadata typically falls into one of the following categories:

- **Descriptive:** This is metadata that describes the elements and nature of a piece of digital content.
- **Structural:** Metadata that provides information about the structure of digital data, such as headers, chapters, pages, etc.
- **Administrative:** Information that makes it easier to manage a specific digital resource. This could include data about the type of resource or access permissions related to the content.
- **Statistical:** Sometimes also called process data, this metadata provides information about statistical data, specifically how this data was collected, processed, and produced.
- **Reference:** Related to the previous entry, this metadata provides information regarding the nature, content, and quality of statistical data.

When we look at digital evidence, such as a Facebook post or tweet, metadata typically provides information on the following:

- **Client Metadata (who collected it)**
  i.e Browser, operating system, IP address, user
- **Web Server/API Endpoint Metadata (where and when it was collected)**
  i.e URL, HTTP headers, type, date & time of request and response
- **Account Metadata (who is the owner)**
  i.e Account owner, bio, description, location
- **Message Metadata (what was said when)**
  i.e Author, message type, post date & time, versions, links (un-shortened), location, privacy settings, likes, comments, friends

We are all familiar with what a typical tweet or post looks like in a social media feed; it looks fairly simple. In most cases, there is some text, an image, and a link. But on the back-end is a lot of information. Here's what the metadata for a short, simple tweet with a static image looks like.


```
"created_at": "Wed Sep 28 22:38:50 +0000 2016",
"id": 781261916362661900,
"id_str": "781261916362661888",
"text": "We're so pleased to celebrate our 1250th customer, Lee County (FL) joining us for #SocialMedia archiving
Cheers! https://t.co/p08shgscLu",
"truncated": false,
"entities": {
  "hashtags": [
    {
      "text": "SocialMedia",
      "indices": [
        82,
        94
      ]
    }
  ],
  "symbols": [],
  "user_mentions": [],
  "urls": [],
  "media": [
    {
      "id": 781261915276410900,
      "id_str": "781261915276410880",
      "indices": [
        114,
        137
      ],
      "media_url": "http://pbs.twimg.com/media/CteZkpiXgAAGUUV.jpg",
      "media_url_https": "https://pbs.twimg.com/media/CteZkpiXgAAGUUV.jpg",
      "url": "https://t.co/p08shgscLu",
      "display_url": "pic.twitter.com/p08shgscLu",
      "expanded_url": "https://twitter.com/PageFreezer/status/781261916362661888/photo/1",
      "type": "photo",
      "sizes": {
        "medium": {
          "w": 700,
          "h": 463,
```


So why is this hidden data important? Generating a hash value when collecting and processing a piece of digital evidence is crucial, but as a best practice, legal teams also want to collect as much metadata as available. Not only does this make it even harder for an opposing party to question authenticity, but metadata can even assist in proving authorship. In other words, metadata can go some way towards showing that an individual was responsible for a particular social media post at a particular moment.

"metadata can go some way towards showing that an individual was responsible for a particular social media post at a particular moment."

In Mining Metadata: The Gold Standard for Authenticating Social Media Evidence in Illinois, Linda Greene makes the following argument:

> *Suppose the Assistant State's Attorney has found the smoking gun in a murder case: an inculpatory statement posted on what appears to be the defendant's Facebook profile. The problem is that the defendant denies that she authored the statement—her account must have been hacked. Fortunately, Facebook records reveal the internet protocol (IP) address of the computer used to create the post, which is then linked to a device within the defendant's exclusive control. In this instance, metadata—the data describing the Facebook transmission—becomes an "elegant weapon" to defeat an otherwise irrebuttable claim. And unlike social media users, metadata does not lie.*

While a hash value might be enough to authenticate a piece of evidence under FRE 902(13) and 902(14), it's important not to overlook the value of metadata. Rather than simply proving that a copy of a social media post looks exactly like the original that appeared on the platform, metadata offers additional insights that make it much harder to deny authenticity.

For this reason, Linda Green argues in her paper that metadata should be the standard when it comes to authenticating digital evidence from sources like social media and websites:

> *This Comment advocates for the use of metadata as the best method of authenticating social media evidence and argues that this method should be adopted as the standard practice in Illinois. Not only is the method endorsed by Illinois courts, and by most courts writing on the subject, but using metadata to authenticate is effective in rebutting the most common challenges to authenticity. Metadata offers conclusive evidence of the accuracy of a copy, as well as convincing circumstantial evidence of authorship. Moreover, collecting metadata for use in authentication is feasible, reduces costs, and provides collateral benefits.*

"Metadata offers conclusive evidence of the accuracy of a copy, as well as convincing circumstantial evidence of authorship. Moreover, collecting metadata for use in authentication is feasible, reduces costs, and provides collateral benefits."

Collecting Self-Authenticating Digital Evidence

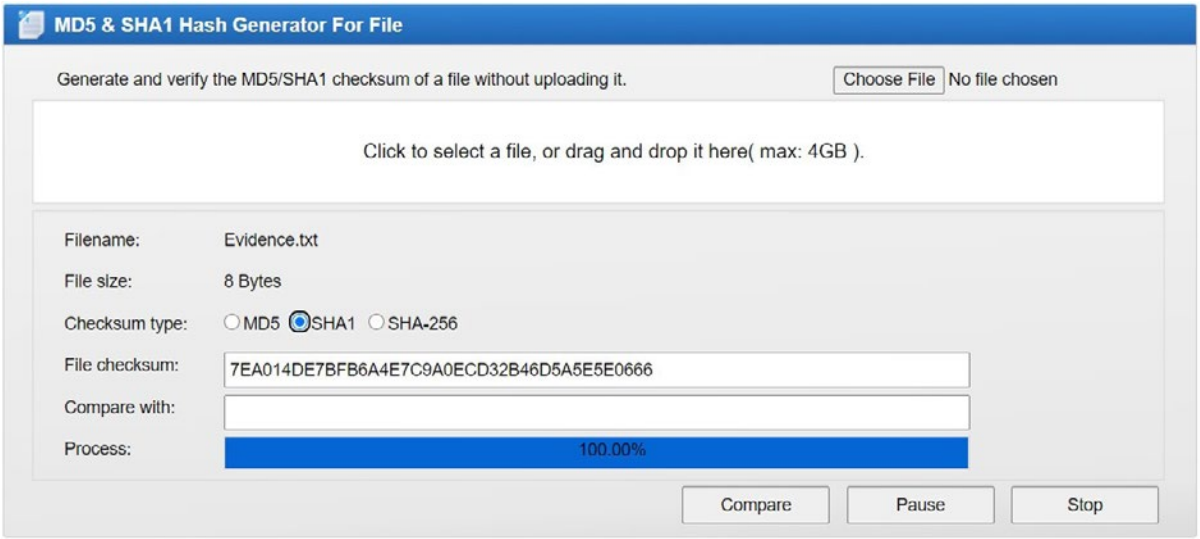
In this section, we will examine how self-authenticating evidence can be collected and preserved. We'll start by looking at how a digital signature, or hash value, is generated.

Generating a Hash Value

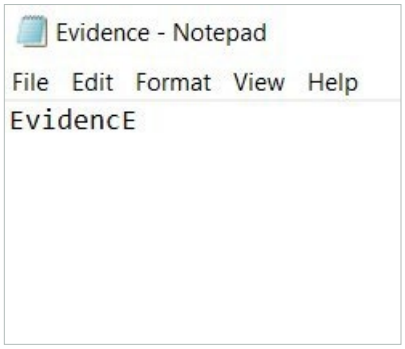
To generate a hash that's associated with a particular file is fairly easy, and can be done with an online tool like OnlineMD5 in a few simple steps:

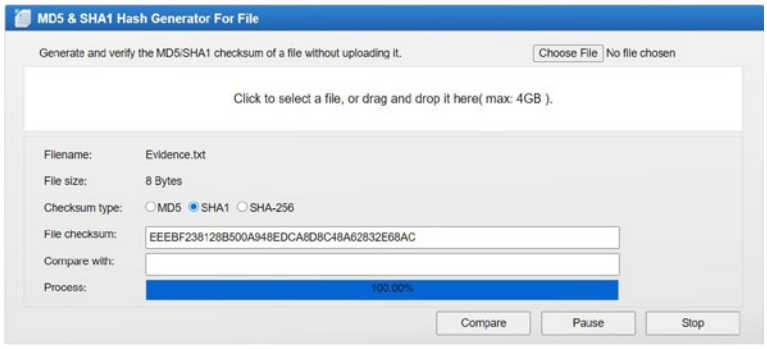
1. Visit http://onlinemd5.com/
2. Select the file that you want the tool to generate a hash for
3. Choose the hashing algorithm you want to use (MD5, SHA1, SHA-256)
4. The hash will automatically appear under "File checksum"

As a test, you can create a simple Notepad .txt file with just the word "Evidence" in it. If you drag it into OnlineMD5 and select SHA1 as the hashing algorithm, the resulting hash will be: 7EA014DE7BFB6A4E7C9A0ECD32B46D5A5E5E0666



Any change to the text file will change the resulting hash value, even simply capitalizing the final letter.





If you then change the content of the .txt file back to simply contain the single word "Evidence", the hash will once again be the one mentioned above.

Ensuring ESI Is Self-Authenticating

The above being said, it is worth adding that using a simple online tool to generate a hash value yourself is probably not advisable. Discussing FRE 902(13) and (14), digital forensics expert La Tonya Williams states, *"the amendment allows the data to be self-authenticating, when best practices are employed and verified and confirmed using hashes and written certification."*

Consequently, to ensure that a court accepts digital evidence as self-authenticating, legal teams should make use of an experienced technician or service provider that:

- Has the knowledge and tools to collect digital evidence while maintaining chain of custody, providing a digital signature (hash value), and capturing associated metadata
- Can certify, through a declaration, affidavit, or letter of attestation, that the evidence was correctly captured

Williams continues to say that not doing the above places a legal team at risk of accidentally spoliating evidence or missing useful metadata that should be included. She argues that:

> *A custodian or their IT professional may not possess the knowledge of how to collect data in a manner that avoids spoliation of file contents and its metadata. Furthermore, they may not possess the tools necessary to produce the authenticating hash values. Also, it is important to keep in mind that the Windows copy & paste function, often used to copy relevant files from one location to another, or a screen print of posts and images on social media sites are not forensically-sound practices. The copy & paste function can alter pertinent metadata (e.g., created, accessed, and modified dates) and simple print screen captures do not collect the associated metadata (e.g., posting creation and edited dates and times). Therefore, careful consideration must be given when deciding if self-collection is worth the price of inadmissibility of crucial evidence.*

"Also, it is important to keep in mind that the Windows copy & paste function, often used to copy relevant files from one location to another, or a screen print of posts and images on social media sites are not forensically-sound practices."

The Sedona Conference Primer on Social Media, Second Edition also mentions the authentication risks associated with self-collection of static images (screenshots and PDFs). Although the paper concedes that these static images will sometimes be accepted by a court, it adds that the loss of metadata can lead to authentication challenges:

> *Some practitioners resort to capturing static images of social media data (i.e., screen shots and PDF images) as a means of preservation, with courts often permitting the use of such evidence at trial. Printing out social media data has its evidentiary limitations, as a static image does not capture the metadata of the image, other than whatever information may be viewable as part of the screen shot. As a result, static images may result in an incomplete and inaccurate data capture that is hard to authenticate, except on the basis of the personal knowledge of a witness. Social media may also contain data and content, such as video, that cannot be properly collected in the form of static images.*

Taking a Best Practices Approach

As stated in the introduction of this white paper, making use of a collection and preservation method that proves the authenticity of a piece of evidence is crucial—and failing to do so will, now more than ever, encourage opposing counsel to question the authenticity and admissibility of that information.

Old collection methods, like taking a simple screenshot of a webpage or social media post, have no place under FRE 902(13) and (14). Legal teams should instead make use of modern tools and solutions that:

- Can capture online media like YouTube and Instagram videos
- Automatically furnish a piece of collected content with a digital signature
- Capture associated metadata
- Collect evidence in a way that makes it easily searchable
- Offer multiple export formats (complete with hash values and metadata)

By leveraging modern solutions, legal professionals can not only benefit from the streamlining and time-saving offered by Amendments (13) and (14), but also improve the overall quality of their digital evidence.

Software Examples

New dedicated legal and eDiscovery solutions make it easy for even small legal and investigative firms to gain access to high-quality defensible evidence. The second edition of the Sedona Conference Primer on Social Media mentions vendor services as increasingly offering opportunities for improved efficiency and reduced cost.

Technology to preserve, collect, and review social media continues to adapt to new services and social media offerings. Similar to early generation email review, where slow and relatively simple technologies were rapidly supplanted by a variety of sophisticated email review options, eDiscovery tools addressing social media will undoubtedly grow in capacity and capabilities and should in the future be able to handle more of the challenges that social media poses.

The primer specifically also mentions evolving technologies that offer the dynamic capture of online data.

Dynamic capture can assist with the preservation and collection of social media. This process captures and analyzes the resulting digital materials based on specific business rules. This analysis allows a party to draw conclusions about the data set based on the rules applied to the data, without corrupting the data.

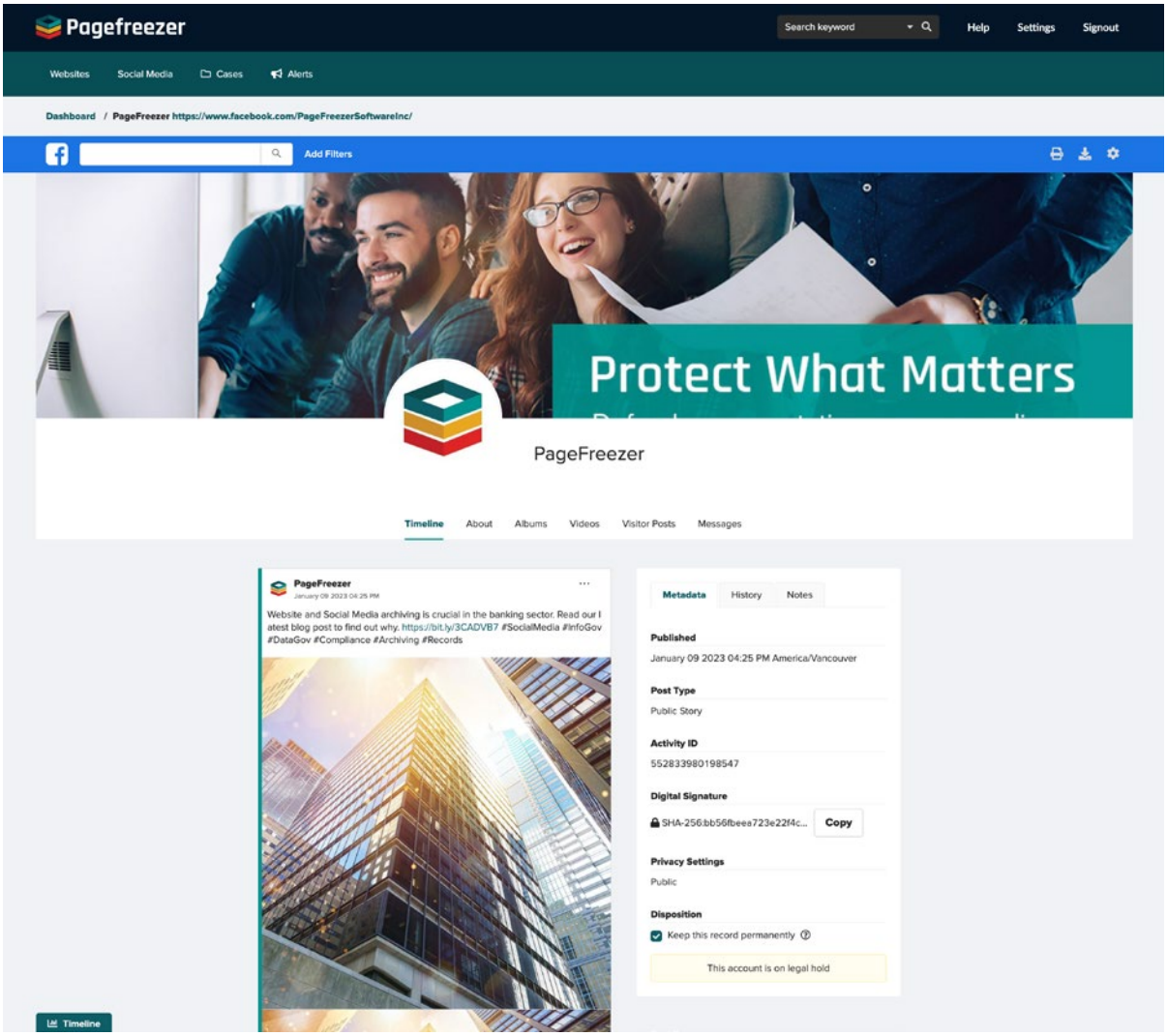
In litigation, dynamic capture processes can be applied to interactive content in cloud-based collaboration sites that needs to be preserved and reviewed. It may also apply to situations involving large amounts of user data on a social media site.

Dynamic capture allows a vendor to identify relevant data in the collaboration site or capture interactive data on the social media site. It then creates data sets that can be reviewed and searched to identify relevant data for litigation without altering it.

Moreover, these solutions extend beyond website, social media, and email content, to also include sources such as mobile text messages, instant messaging tools, and team collaboration tools (like Slack, Microsoft Teams, and Workplace from Facebook).

As an example, a solution like Pagefreezer offers the automated real-time collection and preservation of websites, social media, text messages, and team collaboration tools. It is ideal for in-house counsel and eDiscovery professionals who want to proactively collect and preserve their organization's online content for possible use during litigation.

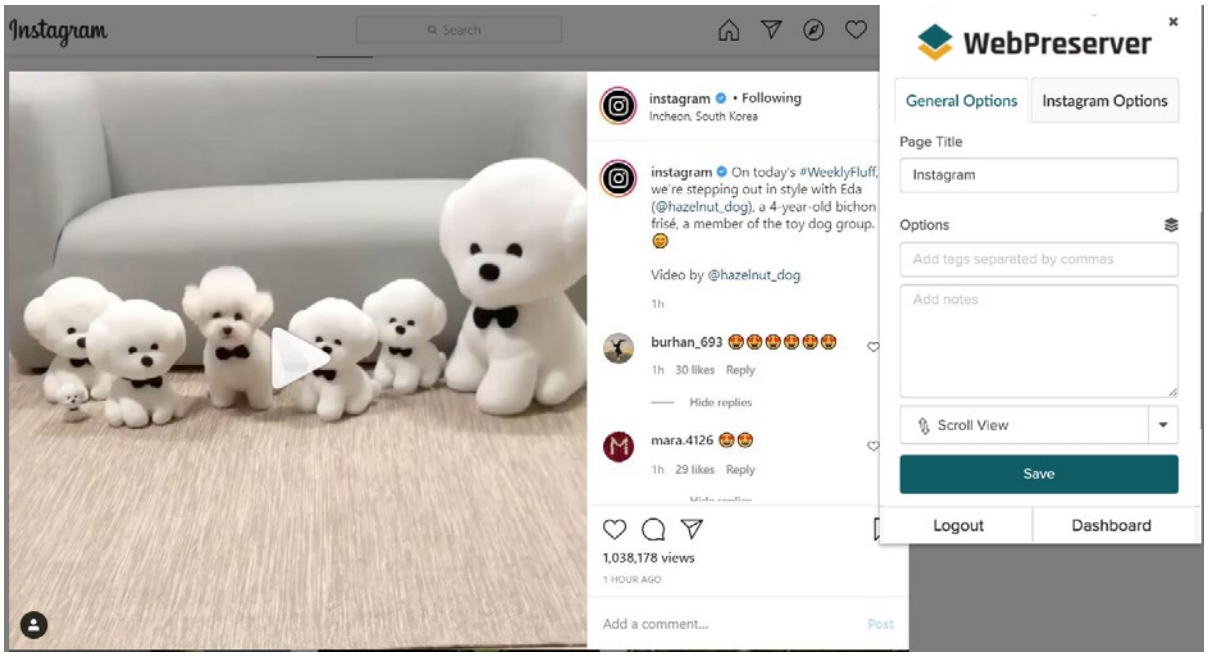
All content is archived automatically, and can easily be searched and exported through a user-friendly dashboard. Associated metadata is captured and each record is automatically given a SHA-256 digital signature. If needed, a record can easily be exported (complete with metadata and has value) to PDF, and then submitted as defensible evidence.



Pagefreezer provides the dynamic capture of online content like websites and social media accounts. All records (including edited posts and deleted content) can be viewed through a dashboard, and instantly exported as defensible evidence.

For investigators and legal teams looking to collect and preserve the website and social media content of a third party, WebPreserver offers the instant one-time capture of dynamic web content through a Chrome extension. All collections are made directly through the browser (not through an API tool), and files are stored on the local computer.

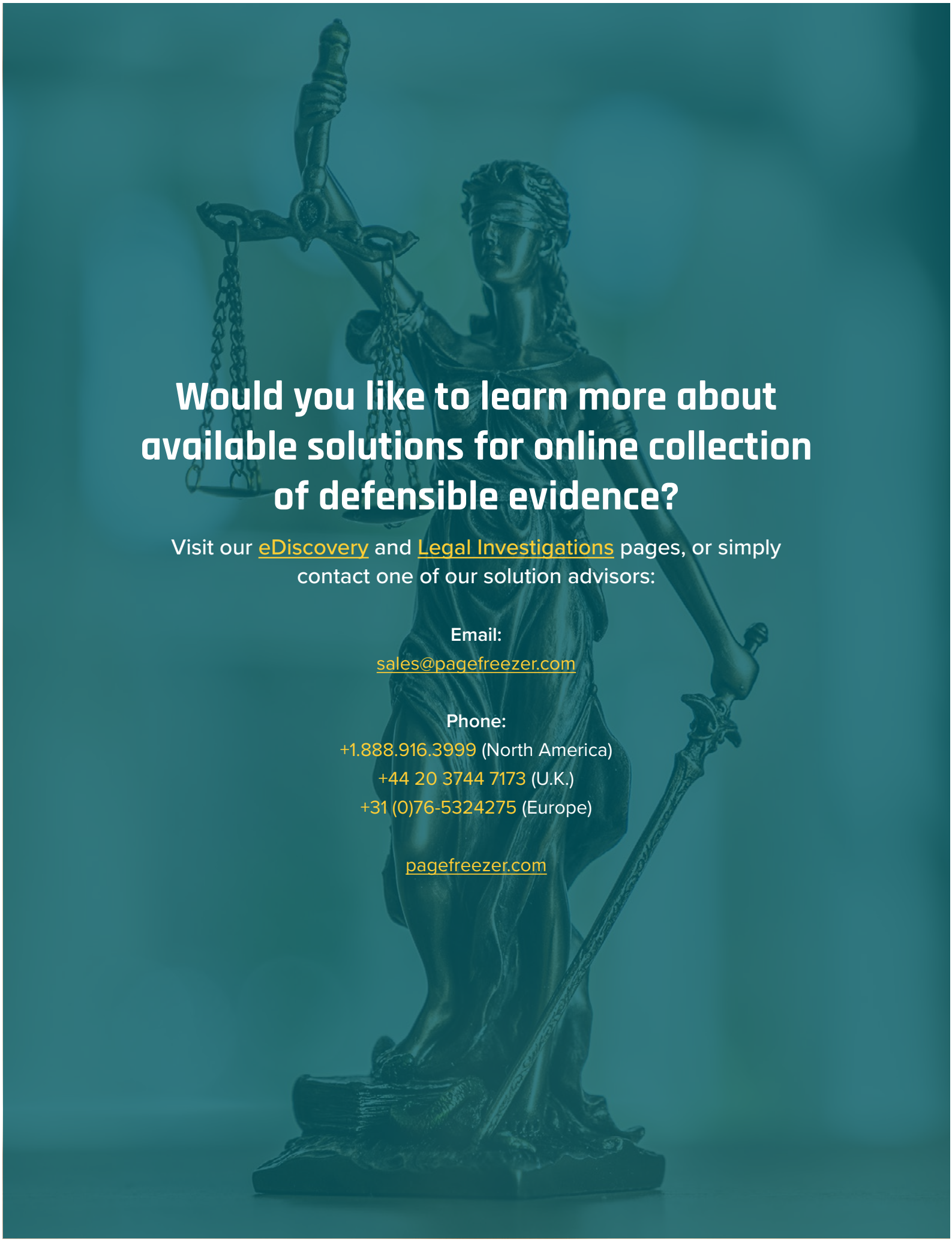
WebPreserver allows a webpage or social media post to be collected and preserved with two simple clicks, or alternatively, bulk captures can be made to automatically collect entire websites and social media timelines. WebPreserver can even collect videos from sites like YouTube and Instagram, complete with their comments.



WebPreserver allows for the collection and preservation of social media with two simple clicks. It will also scroll through timelines and expand comments automatically.

New tools, like those mentioned above, give legal teams and eDiscovery professionals the ability to collect and preserve self-authenticating evidence under FRE 902(13) and (14)—and to greatly streamline their evidence collection in the process.

Taking screenshots of social media pages and websites is a frustrating, time-consuming exercise—and ultimately, the admissibility of that collected evidence remains questionable at best. New technology solutions make it easier to authenticate evidence under Amendments (13) and (14), and also much simpler and easier to collect and preserve it. By leveraging new solutions, legal teams can reduce manual collection work, improve the quality of their evidence, and do away with the need for an expert witness every time a piece of digital evidence needs to be submitted.



Would you like to learn more about available solutions for online collection of defensible evidence?

Visit our eDiscovery and Legal Investigations pages, or simply contact one of our solution advisors:

Email:

sales@pagefreezer.com

Phone:

+1.888.916.3999 (North America)

+44 20 3744 7173 (U.K.)

+31 (0)76-5324275 (Europe)

pagefreezer.com