Best Practices for Preserving Social Media Evidence

There is a big difference between documenting social media evidence with screenshots, or a PDF, and actually preserving the social media as evidence in accordance with the best practices.

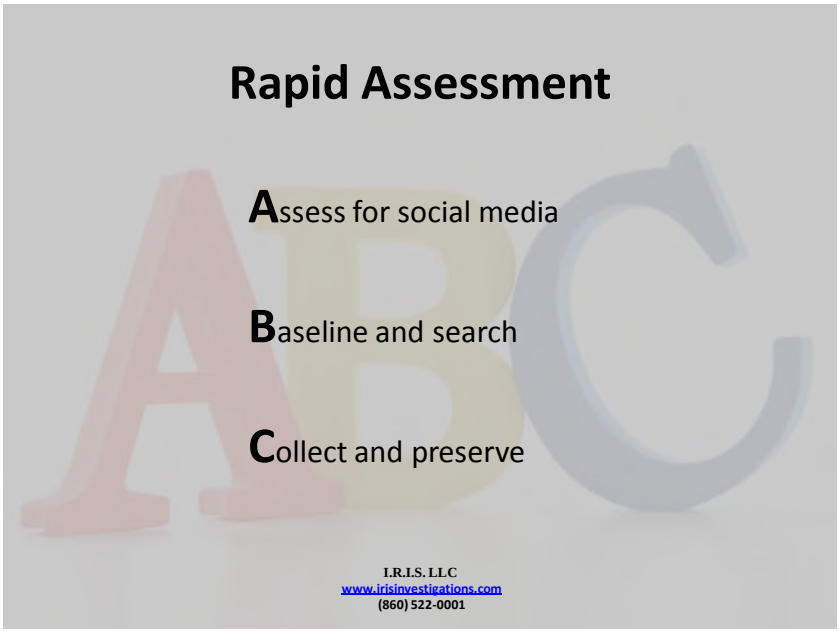
Unlike other forms of evidence, preserving social media has a lot of logistical challenges: It is fluid and time sensitive. It could contain posts, images, videos and active content that have associated metadata. It requires a process to document what was done and preserve what was discovered. It must meet the best practices and overcome questions of admissibility.

In our earlier post on this topic, *Best Practices for Searching Social Media for Evidence*, we described a universal approach for searching the internet for social media evidence. In this article we will discuss the best practices for preserving social media evidence, the rules of evidence that apply and steps that can be taken to overcome anticipated admissibility issues.

"Social media evidence can have a direct impact on the outcome of a case"

Internet and social media evidence is not only useful in family and criminal litigation, but can influence personal injury, workers' compensation, product liability, commercial litigation, and employment cases.

The key is to rapidly assess each case for potential social media sites to be searched and to make sure that you're accessing the information in a permissible and ethical manner. And that the evidence is preserved in accordance with the best practices.



GETTING STARTED

As we described in our previous post *Best Practices for Searching for Social Media for Evidence*, every situation should be assessed early on for possible sources of social media and internet evidence by the involved parties, first degree associates, witnesses and the scene itself. The searches will be conducted simultaneously on search engines like Google, Yahoo and Bing, as well as, specific social media platforms. The search for social media evidence should also include the scene or geographical area. The following example shows the results of a Twitter search by geographical area.

The approach should use a combination of open source and platform searches, documentation of the findings using print screens pasted into a word document, or saving the pages as a PDF as you go.

Basic Steps to Preserve Social Media

When a social media search is conducted as a general background search or to identify or locate witnesses, advanced preservation methods are not always needed.

- Documenting the methods used to conduct the searches should include site URL.
- It should include a screenshot of the home page.
- It can be saved as a PDF for future reference.
- When using credentialed accounts a signed consent form should be obtained.

While this approach is acceptable for documenting the methods used to search and report the findings such as the URL address of the Facebook page, or a photo of the person for identification, this process is not considered the best practice for the actual preservation of social media as evidence because of potential reliability and admissibility issues. The basic steps do not capture metadata, imbedded video or active content, such as newsfeeds, and an advanced process is needed to preserve these items properly.

Advanced Preservation Methods

The advanced process should capture the entire page to include the metadata as well as imbedded images and videos along with active content. These extra steps are needed to overcome admissibility issues such as ownership and authorship. For example, obtaining the metadata of a particular page could identify the owner of the site. Advanced methods of preserving social media evidence can get more information than basic searches, including metadata that could be needed later. The process should be conducted by trained personnel and in accordance with a quality management system used by the scientific community. This quality system ensures repeatable and reliable results.

The most effective way to preserve evidence from the internet and social media accounts is through a forensic approach that will help account for the chain of custody, authentication, admissibility and hearsay issues. The admissibility challenge will still include establishing ownership and authorship of the information in question.

All electronically stored information must meet certain standards before it can be admitted as evidence. A framework for the admission of electronically stored information was established by Judge Paul Grimm in Lorraine v. Markel American Insurance Co. that now serves as a guideline for the admission of electronically stored information into evidence based on the Federal Rules of Evidence.

New amendments to FRE 902 became effective December 1, 2017:

- Rule 902 (13) provides for self-authentication of records "generated by an electronic process or system that produces an accurate result" (for example, a system registry report showing that a device was connected to a computer).
- Rule 902 (14) provides for self-authentication of records "copied from an electronic device, storage medium, or file" (including email and other user-created records) that can be authenticated using the documents' respective "hash values."

Additionally, the electronically stored information provided should either be an original or considered as an admissible duplicate based on FRE 1001–1008. This is often called the best evidence.

When speaking of metadata any printout or duplicate of such information would be admissible “so long as it accurately reflects the data.” (Lorraine, 241 F.R.D. at 578.) Any computer printout of such information that has been certified is admissible. (Norton v. State, Ala. Crim. App. 1987).

Finally, the probative value of electronically stored information must not be “substantially outweighed” by “unfair prejudice” or any other consideration embodied in FRE 403.

Digital Evidence Admissibility

Legal Guidance	*Subject*
Federal Rules of Evidence 104(a)	Preliminary Questions; relationship between judge and jury
Federal Rules of Evidence 104(b)	
Federal Rules of Evidence 401	Relevance
Federal Rules of Evidence 402	
Federal Rules of Evidence 901	Authenticity; including examples of how to authenticate
Federal Rules of Evidence 902	Self-Authentication; including examples
Federal Rules of Evidence 801	Hearsay; including exceptions to the hearsay
Federal Rules of Evidence 803	
Federal Rules of Evidence 804	
Federal Rules of Evidence 807	
Federal Rules of Evidence 1001 through 1008	Original Writing Rule; also known as the “Best Evidence Rule.” Includes use of accurate duplicates.
Federal Rules of Evidence 403	Balance of Probative Value with Unfair Prejudice

So when it comes to using social media as evidence, all the usual standards apply:

1. Is it relevant?
2. Is it authentic?
3. Is the chain of custody established?
4. Is there a hearsay problem or exception?

1. Relevancy

Trail v. Lesko

The question of relevancy in this matter dealt with accessing a Facebook account to get specific posts during discovery. A requesting party must show "sufficient likelihood" that such an account would include relevant information that is "not otherwise available" before being granted access to it.

What it really comes down to is:

- Can you legitimately access the account and show that it is contradictory to what the party is claiming?
- Is it relevant information?

2. Authenticity

In order for the social media evidence to be admissible, you have to be able to show not only that the person owns the account, but that they authored the post in question.

Maryland Standard (Griffin v. State)

The judge is the gatekeeper for the evidence and the jury makes the final decision as to the reliability of that evidence.

Texas Standard (Tienda v. State)

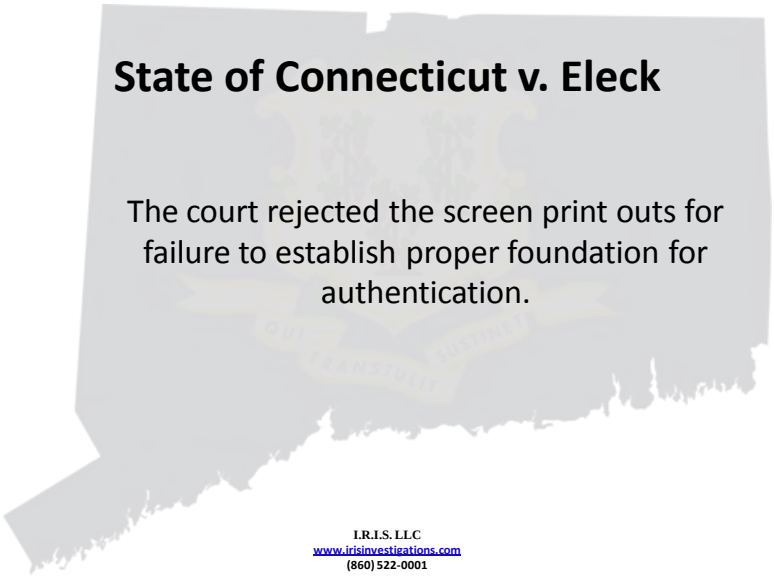
Social media evidence may only be authenticated through testimony from the creator of the social media post; hard drive evidence or internet history from the purported creator's computer; or information obtained directly from the social media site itself. In most cases what's needed is to be able to show appropriate circumstantial evidence.

Pennsylvania's 3rd Circuit Court of Appeals on U.S. v. Brown

This recent case used the Texas standard. Social media evidence is not self-authenticating, even with a certificate from the site. You have to use circumstantial evidence and the standard is preponderance.

State of Connecticut v. Eleck

In Eleck, a post from a witness's social media account was used in the form of a screenshot. The witness denied she made the post and claimed her account was hacked. There was no other proof offered other than the screenshot offered to authenticate who sent the message.



Solutions in CT v. Eleck

1. Automated process of preserving the entire account in PDF which can show supporting circumstantial evidence and help to show authorship
2. Validate with file level hash value
3. Preserve the evidence using advanced methods
4. From a search of the device that created the evidence

Griffin v. State, 419 Md. 343, 19 A.3d 415 (Md. Ct. App. 2011),

The court overturned a conviction because MySpace pages of the defendant's girlfriend, on which there were threats against a key witness, lacked a proper foundation as they were not properly authenticated. The court analyzed a Maryland rule of evidence that was, in part, similar to FRE 901 and looked at decisions in other states. The court held that the prosecutor's effort to authenticate through the police officer rather than the girlfriend, who testified at trial, was insufficient. The court noted that the prosecution could also have searched the computer of the person who allegedly created the profile and the posting or sought information from the social media website.

The Texas Court of Criminal Appeals in Tienda v. State

The court noted that the Griffin methods of authentication are reliable, but that different combinations or amounts of circumstantial evidence may also be sufficient. While the three Griffin guidelines still require evidence of a social media profile to be proven, Tienda sets a slightly lower standard for authentication, requiring only that a jury could reasonably find the evidence to be authentic.

FRE 901(b) gives examples of how authentication can be accomplished. Generally, the proponent of the internet printout must provide testimony by live witness or affidavit that the printout is what it purports to be.

State of Texas v. Tienda

Prosecution used social media evidence based on circumstantial evidence:

User name associated with his nickname and email addresses registered to the user account,
User ID number
Stated location
Communications with others
Posts including time stamps
Associated metadata

I.R.I.S. LLC
www.irisinvestigations.com
(860) 522-0001

3. Chain of Custody

Documentation and Authentication

Documentation of digital evidence incorporates the twin issues of authentication and chain of custody. A key issue in authenticating digital evidence often involves establishing the identity of the author of the electronic records.

Federal Rules of Evidence, also adopted by many state courts, allow that authentication may be established via testimony of a knowledgeable witness, such as a law enforcement officer who seized a computer and a cell phone expert who is able to testify where the files were taken from and matches the names in the files to other evidence collected.

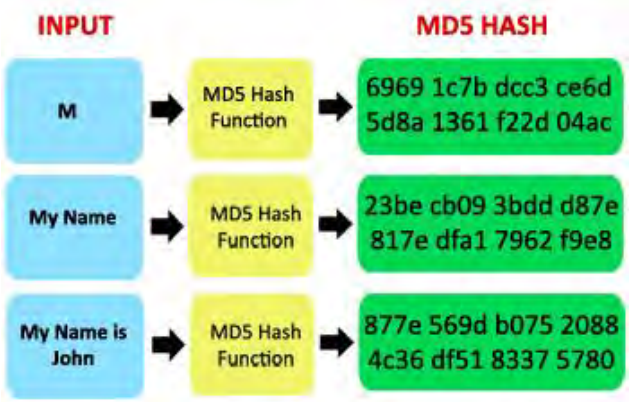
As part of the authentication process, chain of custody assures that digital evidence has been preserved in its original form. This means being able to document when the evidence was collected and where it was collected from (i.e. type, identity, and ownership of device), who owned the device, and who had access to it. It also entails how the evidence was collected (i.e. what tools and procedures were used). Finally, chain of custody involves documenting how the evidence was stored, who has handled the evidence, and who had access.

When trying to admit profiles from social media sites, other factors must be considered. Because anyone can make a profile under any name on these sites, additional circumstantial information is necessary to authenticate social media messages. Simply being marked as "sent from" a particular profile is not enough, as profiles can be hacked into or used without permission.

Hash Values

Hash values are a useful tool for the authentication of electronic evidence. A hash value is an alpha-numeric value of a fixed length that uniquely identifies data. Think of a hash value as an evidence seal. Just like if the evidence seal is broken, if the original file is changed or modified it will no longer have the same hash value.

There are many file hashing algorithms. A common method of authenticating electronic files is through use of Message Digest 5 (MD5) hash value. The following image is an example of a text document that was created where "M" and a hash value was generated. If the same file was modified and content changed to "MY NAME" and then "MY NAME IS JOHN", a hash value would change every time the file is modified.



4. Hearsay

After the evidence has been authenticated, it must be determined not to be hearsay. There are many exceptions to the hearsay rule, and digital evidence often is exempted under one of these exceptions. One exception to the hearsay rule is an opposing party's statement (Federal Rules of Evidence 801[d][2])—for example, statements made by the defendant that are preserved in text messages, email, or other digital media.

Also, a statement is defined as "a person's oral assertion, written assertion, or nonverbal conduct."-Fed. R. Evid. 801(a). Therefore, metadata and geotagging cannot be hearsay because they are not statements made by a person. (Lorraine, 241 F.R.D. at 564.) Several courts have upheld this distinction, including the United States Tenth Circuit Court of Appeals, which held that a computer generated "header" was not hearsay because the information was automatically generated by a computer without any input from a person.

The method and manner in which the evidence was discovered and preserved can make all the difference in admissibility and authentication issues.

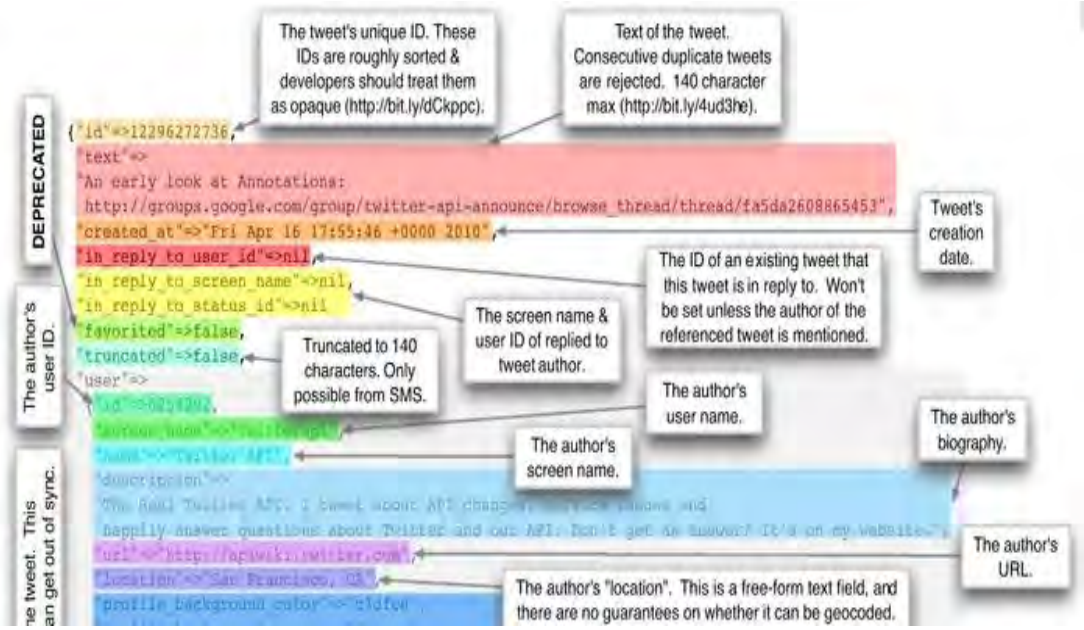
PRESERVATION

Preserving internet and social media evidence with a simple screen capture may be the easiest, but doesn't address the admissibility of the data and doesn't capture the page code metadata that helps establish ownership. It also does not capture the imbedded videos or active content. Keeping a hard copy or PDF copy is another quick and easy method of preservation, but it also comes with limitations. It does not capture the page code metadata that actually makes up the content of the website or imbedded videos.

<u>What is Metadata and why is it important</u>

Metadata is the data about the data. Social media sites provide metadata fields that help tie the user to the evidence. These fields include post creation time, all the recipient names of a sent message, the application or device used to post the evidence, and the user's account ID. Obtaining the metadata can be critical in revealing information that could go to show ownership and location data.

The following example is the metadata of a tweet.



Open Source Tools

Some open source tools can download complete websites and organize the information for the user, saving time and money. However, there is a steep learning curve and it can be difficult to view the material and get it to display as it would in a browser.

Advanced Tools

Developed specifically for web-content preservation, they allow users to capture single pages or social sites in their entirety, and will even gather metadata, such as location information on where posts were made. Users can also schedule ongoing collections. And, you can run keyword searches on the collected content, tag a post or comment on a post and export single artifacts without having to export that entire account.

Subpoenas

Most of the social media providers are based in California and they will want a local subpoena. They will claim that sharing the information violates the Stored Communications Act (SCA). They won't respond to a subpoena for the content itself. They may provide proof of ownership of the account.

The majority of courts hold that internet service providers and social media websites are electronic communications service providers bound by the SCA to not produce postings and emails of their subscribers/registrants in response to a civil subpoena. Instead, the party seeking discovery could use Rule 34 which requests the opposing party to obtain the postings. To obtain social media postings of a non-party witness the best practice is to serve a subpoena on the non-party, not the social media ISP.

Check the Terms of Service for the social media website as they may have an impact on your approach to obtaining the information or even the target of your discovery demands. In People v. Harris, a criminal prosecution of an Occupy Wall Street protestor, the prosecutor served a subpoena on Twitter. The court denied defendant's motion to quash (36 Misc.3d 613, 945 N.Y.S.2d 505 (2012)) because he lacked standing. Twitter then moved to quash; the court again denied (36 Misc.3d 868, 949 N.Y.S.2d 590 (2012)) and held that the defendant had no proprietary interest or expectation of privacy in his tweets and that by submitting tweets he had granted Twitter an unlimited license to use and distribute the tweets.

Admissibility

An important evidentiary issue with respect to digital evidence is reliability. The Federal Rules of Evidence 702 requires that scientific and expert testimony must be reliable, both with respect to the principles and methods used by the expert, and application of the principles and methods to the specific facts.

Reliability & Repeatability

Daubert held that the courts have a gate keeping obligation to assess reliability of scientific evidence. The Supreme Court proposed five criteria to determine the admissibility of scientific evidence: whether the technique has been tested, whether it has undergone peer review, whether there is a known error rate, the existence and maintenance of standards controlling its operation, and (like Frye) whether the technique is generally accepted by the scientific community.

ISO 17025
ACCREDITED LABORATORY

The ISO 17025 standard meets the requirements under Federal Rules of Evidence 702. It states that scientific and expert testimony must be reliable, both with respect to the principles and methods used by the expert, and application of the principles and methods to the specific facts. This standard relies on a quality system of documentation and practices that ensures reliability.

- Written quality manual
- Written technical procedures
- Documented equipment testing and validation
- Documented examiner proficiency

CONCLUSION

Preservation of social media evidence is time sensitive and should begin as soon as possible. It needs to meet the industry standards by being repeatable and reliable. It must establish the chain of custody, create data hash values and include not only the entire site, but the page code metadata, the embedded photos and videos, and the active content.

A defined set of best practices and industry standards exists governing the preservation and analysis of internet and social media evidence.

The U.S Department of Justice - National Institute of Justice (NIJ) has published a comprehensive Special Report titled Investigations Involving the Internet and Computer Networks.

The Industry Standards/Best Practices and other informational materials are available on our website in our Digital Evidence Toolbox

Minimum Standards

- ✓ **Experienced & Certified**
- ✓ **ISO Quality System**
- ✓ **Meets Industry Standards and Best Practices**
- ✓ **Chain of Custody**
- ✓ **Data Hash Values**
- ✓ **Capture Entire Sites**
- ✓ **Associated Sites**
- ✓ **Imbedded Photos and Videos**
- ✓ **Metadata**
- ✓ **Location Data**

CONTACT US

Have questions or need help on a case? Our team at I.R.I.S. LLC consists of experienced, cross-trained investigators that regularly conduct searches for internet and social media evidence. We provide training to other professionals and organizations. We have the tools and expertise to preserve digital evidence using a forensic approach meeting the industry standards and best practices.