Authentication and Admissibility of Digital Evidence

Jeff Welty

UNC School of Government

May 2026

Introduction

Digital evidence is everywhere. A victim testifying in a misdemeanor communicating threats case may pull out her phone to display a text message from the defendant. In a family law matter, one spouse's private investigator may seek to play a digital video he recorded of the other spouse dining with a paramour. In a murder trial, the prosecution may offer a social media post showing the defendant with a gun as evidence of the defendant's access to firearms.

This paper is intended as a brief summary of current law related to the authentication and admissibility of digital evidence. A few preliminary comments: First, the paper does not address the acquisition of such evidence, which in criminal cases sometimes raises important Fourth Amendment questions. Second, many of the cases discussed in the paper are criminal cases. That may be partly a result of the author's background in criminal law, but it is also a function of the fact that many of the appellate opinions in this area arise from criminal matters. Third, the paper draws primarily on cases decided by the North Carolina appellate courts and the Fourth Circuit Court of Appeals, but occasionally cites and discusses cases from other jurisdictions.

The paper focuses primarily on authentication because it is the issue of authentication that is unique to digital evidence. Of course, such evidence may be irrelevant, or contain hearsay, or raise issues of privilege. But those issues are mostly no different for digital evidence than for other types of evidence. Still, a few issues other than authentication are mentioned in what follows when appropriate.

Types of Digital Evidence

Digital evidence comes in many varieties. Some of the common categories are:

- One-to-one messaging (such as emails, text messages, and social media direct messages)
- Social media posts (which may include text, photographs, and/or videos)
- Digital photographs and videos captured by a witness or by a surveillance system (such as a store's loss prevention system)

- Information extracted from a party's electronic device (which may include communications, photos, videos, browsing history, metadata, and much more)
- Location information (such as cell site location information or GPS data from a tracking device)
- Records from internet-based businesses like Venmo or eBay

Some of these categories overlap. For example, a text message may be sent to a witness and also extracted from a defendant's phone after it is seized by police. Records from an internet-based business like Facebook may be used to help authenticate a social media post made by a party. Furthermore, these categories are far from exhaustive. Digital evidence may come from many other sources, such as home smart speakers, automotive safety systems, and fitness trackers.

In some instances, how the evidence is obtained may be just as important as the kind of evidence at issue. The process for authenticating an email may be different depending on whether it is offered through the recipient, through the author, through an expert who found the email in a forensic search of a device, or through an investigator who obtained the email by sending a search warrant to the email provider.

Because this paper is not intended to be a comprehensive treatise, it will focus on the first three categories of digital evidence, which may also be the most common in practice: one-to-one communications, social media posts, and digital photos and videos.

Authentication Generally

The authentication of evidence is governed by the 900 series evidence rules. The state and federal rules are similar. Under N.C. R. Evid. 901(a), "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Authentication may be seen as "a special aspect of relevancy," in the sense that if the evidence in question is not genuine or is not what it purports to be, it will not be pertinent to the dispute at issue. Adv. Comm. Note, N.C. R. Evid. 901.

The burden is on the proponent of evidence – that is, the party seeking to introduce the evidence – to authenticate it. However, the "burden to authenticate . . . is not high – only a prima facie showing is required." State v. Ford, 245 N.C. App. 510 (2016). If the proponent shows that a reasonable finder of fact could find that the evidence is what the proponent claims, the burden of authentication has been met. The opposing party may, of course, continue to attack the validity of the evidence, but such efforts would go to the weight of the evidence, not its admissibility.

Over the years since digital evidence first appeared in the courts, there has been a trend towards more ready acceptance of the admissibility of such evidence. At first, courts tended toward skepticism in light of the possibilities of spoofing or faking digital evidence, but in recent years have been much more willing to admit it. See Christopher B. Mueller & Laird C. Kirkpatrick, 5 Federal Evidence § 9:9 (4th ed. 2025 update) (noting that "[s]ome of the early judicial opinions indicated extreme skepticism" about the admissibility of web content). Whether that trend will continue in the age of artificial intelligence is addressed briefly near the end of this paper.

One-to-One Messaging

One-to-one messages are often introduced in the form of a photograph or screenshot (for example, of an exchange of text messages) or in the form of a printout (for example, of an email). Typically, the witness will testify that he or she made the photograph or screenshot or printout and that it accurately reflects the electronic message itself. This is the first step in the process of authentication: establishing that the exhibit to be offered and the underlying digital content are the same.[1]

The second step in the authentication process normally relates to authorship: is there sufficient evidence to authenticate the writing as having been created by the person the proponent contends did so? Pertinent provisions of Rule 901 include subdivisions (b)(1) (testimony of a witness with knowledge) and (b)(4) (distinctive characteristics).

The easiest case is when the sponsoring witness testifies that he or she is the author of the communication. But courts may also find sufficient evidence of authorship when the sponsoring witness is the recipient of the communication and testifies that it came from a phone number or account regularly used by the alleged author, or that the communication is a part of a larger conversation the witness was having with the alleged author. See, e.g., State v. Gray, 234 N.C. App. 197 (2014) (a photograph of a text message exchange obtained from a robbery defendant's cell phone was authenticated by the testimony of a co-conspirator who testified that the exchange was between the co-conspirator and the defendant and that it concerned the robbery they were planning). Cf. Clark v. Clark, 280 N.C. App. 403 (2021) (in an alienation of affection lawsuit, text messages from the defendant spouse to his romantic partner, including one featuring a sexually explicit photograph, were authenticated by the plaintiff spouse's testimony that "she observed the text messages on [her spouse's] telephone, took a picture of said messages using her

[1] One could also think of this step as satisfying the best evidence rule, N.C. R. Evid. 1002, by showing that the exhibit is either an "original" under Rule 1001(3) or a "duplicate" of the digital content under Rule 1001(4) and therefore admissible under Rule 1003.

cellphone, and matched the phone number [from which the text messages originated] with that of [the romantic partner]").

Similarly, a witness may authenticate the authorship of an electronic communication by showing that the alleged author engaged in conduct consistent with authorship. For example, in United States v. Davis, 918 F.3d 397 (4th Cir. 2019), an officer was using a confidential informant to conduct a drug investigation. The officer watched the informant texting with a drug supplier and took photos of the messages. The supplier's side of the conversation was authenticated as having been written by the defendant based largely on the fact that the texts concerned where to meet for a transaction and the defendant showed up at the meeting place established in the text exchange.

There is no specific formula for what circumstantial evidence will be sufficient to authenticate a message. In State v. Davenport, 297 N.C. App. 605 (2025), a man was charged with murdering his brother. The court found sufficient evidence to authenticate threatening Facebook Messenger communications as having been authored by the defendant where (1) a witness testified that the defendant typically used Facebook Messenger to communicate with others, and specifically that he used Facebook Messenger to communicate with the victim, and (2) the officer who searched the victim's phone and found the messages testified that they came from an account bearing a name similar to the defendant's and that the content of the messages included a reference to being the victim's brother. See also State v. Taylor, 178 N.C. App. 395 (2006) (text messages allegedly from a murder victim to the defendant arranging a meeting were adequately authenticated as having been written by the victim where they referenced the victim's first name and correctly described the car the victim was driving).

Although a majority of recent decisions concerning electronic communications have come out in favor of sufficient authentication, there are cases to the contrary based on the specific facts of those cases. See, e.g., Arnett v. Estate of Beavins by Beavins, 184 N.E.3d 679 (Ind. Ct. App. 2022) (email not authenticated based solely on "a typed signature block" and the fact that it originated "from an email address bearing [the purported author's] name" absent any evidence about "the contents, substance, or other distinctive characteristics of the email" that would support authorship); Armstrong v. State, 607 S.W.3d 491 (Ark. 2020) (text messages offered by murder defendant, allegedly authored by the victim, were not authenticated; the messages were recovered from a phone by a forensic examiner after the murder but there was "no testimony or other evidence . . . to corroborate the sender's identity [beyond the name programmed into the phone as connected to the sending number], and there was also no testimony as to the owner of the phone, where it was found, or who possessed it"); Commonwealth v. Bustard, 275 N.E.3d

118 (Mass Ct. App. 2026) (a Snapchat message was not authenticated where the account name was not similar to the defendant's and the content of the communication did "not refer to any prior conversations between the victim and the defendant" and "contain[ed] no personal references" or any distinctive tone associated with the defendant's communication). In general, it may be difficult to authenticate authorship based only on the fact that a message comes from an account bearing a name similar to the purported author's name. Usually, some additional evidence connecting the purported author to the account is required.

The above addresses messaging that is composed primarily or exclusively of text. Sometimes one-to-one messages are in the form of, or contain, images. The considerations around the authentication of such images are similar to the considerations informing the authentication of images posted on social media, a topic addressed below.

Social Media Posts

The authentication of social media posts is similar to the authentication of one-to-one communications. Like one-to-one communications, a party seeking to introduce a social media post typically will come forward with a photograph, screenshot, or printout of the post. Again it may be helpful to think of authentication as a two-step process. The first step is to establish that the photograph, screenshot, or printout accurately reflects the underlying post. The second step is to show that the post itself is authentic. Usually, the second step requires evidence that a particular person wrote or created the post.

A case that lays out these two steps clearly is State v. Clemons, 274 N.C. App. 401 (2020). The defendant in that case was subject to a restraining order that prohibited him from having any contact with the victim. Shortly after the defendant was released from prison, someone began making comments on the victim's social media posts. The comments appeared through the defendant's daughter's account, but the victim believed that the defendant was the author and she captured screenshots of the comments. The defendant was charged with violating the restraining order, the screenshots were introduced at trial, and the defendant was convicted. The North Carolina Court of Appeals ruled that the screenshots were properly admitted. The framework it laid out was:

> In order for the screenshots of the Facebook comments to support finding Defendant contacted [the victim], the screenshots must have accurately reflected [the victim's] Facebook page. Therefore, the screenshots must have been authenticated as photographs. However, the screenshots of the Facebook comments are also statements—the State wanted the jury to use the screenshots to conclude Defendant communicated with [the victim] in violation of the DVPO . . . .

> The evidence must show Defendant was responsible for the Facebook comments . . . [so] the Facebook comments also needed to be authenticated by evidence sufficient to support finding they were communications actually made by Defendant.

In Clemons, the court found that the first step was satisfied by victim's testimony that the screenshots were accurate, and the second step was satisfied by circumstantial evidence that the comments began appearing shortly after the defendant was released from prison, at a time when the defendant was also contacting the victim by phone, and included content that was typical of the defendant and not typical of his daughter.

As was the case in Clemons, testimony from a social media user is a common way of showing that an offered exhibit accurately represents an underlying social media post. Intemann v. State, 855 S.E.2d 666 (Ga. Ct. App. 2021) (officer testified that he accessed the defendant's Twitter account and printed out Tweets from the account; this "established a prima facie case that the printouts accurately reflected the contents of the Tweets").

Another common way to satisfy the first step in the authentication process is for a party to obtain a certification from the social media company to the effect that the content is a business record of the company. This is particularly common in criminal cases in which an officer obtains the material originally via a search warrant directed at the social media company. The state and federal rules of evidence differ slightly in the details, but in general, both allow a written statement from a custodian to authenticate the records and to establish the applicability of the business records hearsay exception. See N.C. R. Evid. 803(6) (business record status may be established by the testimony of a custodian, by affidavit, or written document; a party must give advance notice of its intent to authenticate business records in this way), State v. Graves, 296 N.C. App. 414 (2024) (ruling that a Facebook post was properly authenticated as a business record by a certificate from a Facebook records custodian, even though the certificate was not notarized or sworn). See also Fed. R. Evid. 902(11) (addressing authentication by certification of business records), 803(6) (addressing hearsay exception for business records); United States v. Allen, 159 F.4th 625 (9th Cir. 2025) (concluding that Facebook posts were sufficiently authenticated by a custodian's certification; the court further explained how the prosecution "separately authenticated the underlying content" of the posts as having been authored by the defendant through circumstantial evidence such as the profile picture matching the defendant and the account being linked to the defendant's phone number); United States v. Banks, 29 F.4th 168 (4th Cir. 2022) (similar; the accuracy of social media posts was sufficiently authenticated by business record certification, and

content/authorship was sufficiently authenticated by circumstantial evidence connecting it to the defendant).

Turning to the second step in the authentication process, authorship of social media content is often established via circumstantial evidence connected the purported author to the account and/or to the specific post in question. In an early state case, State v. Ford, 245 N.C. App. 510 (2016), the reviewing court found that the defendant's authorship of a social media post was sufficiently authenticated by the fact that the account contained "content unique to defendant" such as pictures of himself, pictures of his dog, and references to his nickname. See also United States v. Recio, 884 F.3d 230 (4th Cir. 2018) (circumstantial evidence authenticated social media content as having been authored by defendant Larry Recio where "(1) the user name associated with the account was 'Larry Recio,' (2) one of the four email addresses associated with the account was 'larryrecio20@yahoo.com,' (3) more than one hundred photos of Recio were posted to the account, and (4) one of the photos posted to the user's timeline was accompanied by the text 'Happy Birthday Larry Recio'); United States v. Azure, 164 F.4th 688 (8th Cir. 2026) (finding sufficient circumstantial authentication of social media post based on the account holder's name and the presence of the defendant's friends as friends on the account).

The majority of recent cases in which the authentication of social media posts has been litigated have found sufficient evidence of authentication. However, examples of insufficient authentication can be gleaned from courts across the country. See State v. Smith, 4136 So.3d 424 (Miss. 2014) (stating that "[t]he ease with which defendants and alleged victims alike could fabricate a social media account to corroborate a story necessitates more than a simple name and photograph to sufficiently link the communication to the purported author" and ruling that there was insufficient circumstantial evidence that the defendant authored social media posts where the defendant's name matched the account in question but "[n]o other identifying information from the Facebook profile, such as date of birth, interests, hometown, or the like, was provided" and the content of the posts concerned matters known to others as well as to the defendant); People v. Kent, 81 N.E.3d 578 (Ill. Ct. App. 2017) (defendant was charged with killing a man in his driveway; a social media post contained the phrase "leave em dead n his driveway" but the court found insufficient circumstantial evidence that the defendant was the author despite the name on the social media account matching the defendant's nickname; the court noted that there was nothing else connecting the defendant to the account); Sublet v. State, 113 A.3d 695 (Md. Ct. App. 2015) (a defendant sought to introduce social media posts purportedly written by an alleged assault victim, but the court ruled that they were not sufficiently authenticated given that she denied writing some of them and testified that she shared her account and password with others).

The foregoing discussion focuses on postings that consist of words or text but many social media posts contain images. Suppose that a party seeks to introduce a photograph that an opposing party or a third party posted on Facebook. What would be required to authenticate the photograph? The proponent's first step would be to show that the printout or screenshot that he or she seeks to introduce as an exhibit accurately reflects what was posted on Facebook. The proponent's second step might depend on the purpose for which he or she seeks to introduce the photograph. For example, if a plaintiff sues a defendant under the disclosure of private images statute, G.S. 14-190.5A, alleging that the defendant posted an electronically altered photograph of the plaintiff that purports to show the plaintiff engaged in sexual conduct, it would not be necessary to show that the photograph is accurate, but it would be necessary to show that the defendant was the one who posted it – an requirement similar or identical to the authorship issue explored above. On the other hand, if a defendant is charged with fraud based on allegedly false claims of disability, and the prosecution seeks to introduce photographs of the defendant dancing and riding a motorcycle, it would be necessary to show that the photograph is accurate, but would not be necessary to establish who posted it. See United States v. Vazquez-Soto, 939 F.3d 365 (1st Cir. 2019) (investigators found photographs of the defendant dancing and riding a motorcycle on what appeared to be his ex-wife's Facebook page; absent much evidence that the page really did belong to the ex-wife, the reviewing court analogized the photographs to printed images found lying on a sidewalk; it nonetheless determined that they were sufficiently authenticated by circumstantial evidence, including an investigator's testimony that he recognized the defendant in the photographs and the fact that "the jurors could examine the photographs and rely on their own observations of [the defendant] in the courtroom"). See also United States v. Farrad, 895 F.3d 859 (6th Cir. 2018) (ruling, in a felon-in-possession case, that photographs taken from what seemed to be the defendant's Facebook page, showing "a person who looks like [the defendant] holding what appears to be a gun," were sufficiently authenticated by circumstantial evidence including that "the details of the account match [the defendant]" and "more importantly, the photos appeared to show [the defendant], his tattoos, and . . . distinctive features of [his] apartment, as confirmed by police investigation").

Photos and Videos

The foregoing addresses photographs posted on social media. What follows covers digital photography and videography more generally. Visual digital content may be captured by retail surveillance systems, by officers' body-worn cameras, by romantic partners in the course of sexual activity, by citizens who see something concerning on the street, and in countless other ways. Because video has become the dominant modality for recording, this paper mainly addresses video, but the legal principles apply equally to still

photographs. As discussed below, there are two well-established ways to authenticate digital video and one emerging way. This section will conclude with a brief discussion of the impact of artificial intelligence in this area of law.

The first established option for authenticating digital video is through the testimony of a witness that the video fairly and accurately depicts the events in question and would help illustrate the witness's testimony. This foundation requires that the witness be familiar with the people, places, or events captured in the video, and it results in admission of the evidence for illustrative purposes. This foundation is common when video is captured by a witness to contested events, with law enforcement video from body-worn cameras or from recorded interviews, and for some videos captured by home or business surveillance systems (when someone was present and observed the events that the system recorded). See, e.g., State v. Ramsey, __ N.C. App. __, 922 S.E.2d 176 (2025) ("The State laid a proper foundation for the video by presenting [a witness's] testimony that the video fairly and accurately illustrated the fight as she saw it.").

The second option for video authentication is the so-called silent witness foundation: a witness testifies that the camera was working properly at the time the video was captured. The witness usually will go on to say that the video to be introduced in court is the same as the video originally recorded by the system – in other words, it has not been altered or tampered with. This foundation is common for home and business surveillance systems and results in the admission of the evidence for substantive purposes. See State v. Snead, 368 N.C. 811 (2016) (holding that a regional loss prevention manager for a department store sufficiently authenticated surveillance video from a store by testifying that he was familiar with the store's "industry standard" surveillance system and with the procedure for storing video to be used in a criminal prosecution, even though he was not at the specific store in question on the date of the offense). Although the usual sponsoring witness in these cases is someone with authority over the home or business in question, the court in State v. Jones, 288 N.C. App. 175 (2023), ruled that a home surveillance video was sufficiently authenticated by an officer who testified only that she saw the video on the night in question and that "to her knowledge" the system was working.

School of Government faculty member Danny Spiegel has prepared a chart summarizing many of the North Carolina appellate cases on the above options for authentication. That chart is available at https://nccriminallaw.sog.unc.edu/wp-content/uploads/sites/4/2024/03/Video-Chart-Final-Spiegel.pdf.

The emerging option for authenticating video is as a business record. This option is most pertinent to surveillance video operated by a business, but could potentially apply to video from home surveillance systems that are operated by a business, such as a Ring doorbell

camera. No North Carolina appellate case has yet endorsed this approach to authentication, but cases in other jurisdictions have. See Daniel Spiegel, A New Way to Authenticate Video? State v. Windseth and the Business Records Exception, N.C. Crim. L. Blog (July 24, 2025) (discussing the issue and collecting cases).

The above avenues are not the only possible ways of authenticating video, merely the most common. For example, in State v. Leggett, __ N.C. App. __, 926 S.E.2d 173 (2026), the defendant was accused of repeatedly drugging and raping his wife. She discovered videos of the attacks on his devices and provided them to police. They were admitted at trial and he was convicted. He appealed, arguing that they could not be authenticated: the victim was unconscious during the assaults, so she could not say that the videos fairly and accurately depicted the events, and no witness testified as to the proper operation of whatever device the defendant used to make the recordings. The appellate court nonetheless ruled that the videos were sufficiently authenticated, largely under N.C. R. Evid. 901(b)(4) (distinctive characteristics). The court noted that the victim "recognized distinctive characteristics based upon her knowledge of the people, location, and approximate time of the videos." She was able to recognize "herself in the videos lying on the bed, and identified the location of the videos as her and Defendant's townhouse," and "also recognized the hands, penis, and ejaculation in the video" as the defendant's.

Over the past year or two, questions have arisen about the impact of artificial intelligence on the authentication of digital video. AI video generators have become extremely sophisticated. They can produce deepfakes – videos that depict real people doing or saying things that they never said or did – that are undetectable or nearly so. Given the risk of being fooled by a deepfake, should courts be more skeptical about admitting video evidence? Should the proponent of video evidence be required to establish that the video was not generated by AI? There is not a large body of case law addressing these questions, but so far, courts are continuing to apply the authentication practices set forth above. See Mooney v. State, 321 A.3d 91 (Md. 2024) ("Video footage, like social media evidence, is susceptible to alteration, and the increased availability of new technology, particularly the advent of image-generating artificial intelligence, may present unique challenges in authenticating videos and photographs. . . . Nonetheless, at this time, video footage can be authenticated through vigilant application of existing methods for authentication of evidence."). A party's objection that a particular video or photograph could have been generated by AI, without some reason to believe that the evidence in question likely was generated by AI, is not likely to succeed. See, e.g., Leggett, supra (rejecting a defendant's challenge to the authentication of a video where "Defendant's allusions to the possibility the videos could be altered are not backed by any evidence in the record nor does Defendant make any specific claim to such effect"); State v. Amyda, 2026 WL 221375 (Ia.

Ct. App. Jan. 28, 2026) (unpublished) (a defendant was charged with sexual abuse, which he captured on video; his "speculative claims that the video was a 'deepfake' without any evidentiary support did not raise a genuine question about the video's authenticity").

Conclusion

The legal landscape concerning the admissibility of digital evidence will continue to evolve. Readers with questions are invited to contact the School of Government. Specific faculty members with expertise in this area include the author; Danny Spiegel; and with regard to the impact of artificial intelligence, Kristi Nickodem. We would be happy to hear from you if we may be of service.