Authentication of Digital Communications

(social media content and text messages)

To authenticate digital evidence, the proponent must show that "the [evidence] in question is what its proponent claims." N.C. R. Evid. 901. A party may offer testimony of a "[w]itness with [k]nowledge" that evidence is what it is claimed to be. *See* Rule 901(b)(1). Alternatively, a party may rely on circumstantial factors such as the "distinctive characteristics" of the evidence. *See* Rule 901(b)(4). "The burden to authenticate… is not high—only a prima facie showing is required." *State v. Ford,* 245 N.C. App. 510 (2016).

Authentication of digital communications involves two questions:

1. **Does the exhibit (screen capture, photo, video) accurately reflect the communication?**
2. **Is there reason to believe that the purported author wrote the communication?**

See State v. Clemons, 274 N.C. App. 401 (2020) ("To authenticate [social media] evidence …there must be circumstantial or direct evidence sufficient to conclude a **screenshot accurately represents the content** on the website it is claimed to come from and to conclude the **written statement was made by who is claimed** to have written it") (emphasis added).

The rules of evidence do not apply when addressing preliminary questions such as the authenticity of digital evidence (*see* Rule 104(a)). Thus, the court may consider the substance of the evidence offered or reliable hearsay in determining whether the evidence has been properly authenticated.

The following memory tool may be helpful in thinking about the various types of circumstantial evidence frequently used to authenticate digital communications.

SANDVAT

S is for **"Substance"**
How does the substantive content of the digital evidence itself tend to authenticate it? e.g., does the communication reference a particular event, nickname, or private topic, thereby tending to show that a particular person was the author?

A is for **"Account"**
Is there information about the account (username/login, digital properties, identifying information associated with account profile) that suggests ownership or authorship?

N is for **"Name"**
Is there a name or "handle" associated with the social media account that indicates authorship?

D is for **"Device"**
Who possessed the phone, computer, or device used to make the communication? What is distinctive about the hardware and is there information as to ownership or possession?

V is for **"Visuals"**
Does the webpage or account display photographs or videos that indicate ownership or authorship?

A is for **"Address"**
What can be learned from the IP address, physical address, or email address associated with the communication?

T is for **"Timing"**
When was the communication made? How does this relate to larger questions of chronology?

The following chart gives examples of adequate and inadequate foundations for digital communications. The types of circumstantial evidence used to authenticate the communication are emphasized.

ADEQUATE

Foundation for Digital Communication

***State v. Davenport*, No. COA24-330, __ N.C. App. __ (2025)**

In murder case, **Facebook messages (social media)** were properly authenticated where:

- A witness identified phone (**device**) found at the crime scene as decedent's
- Messages were found on the phone in a message thread under defendant's **name**
- A witness testified that the defendant did not have a phone and communicated with the witness and the decedent through Facebook Messenger app
- **Substance** of messages contained distinctive personal details such as name of decedent's son

***State v. Clemons*, 274 N.C. App. 401 (2020)**

In domestic violence protective order violation case, **Facebook comments made on victim's posts** were properly authenticated where:

- Although the comments originated from the victim's daughter's **account**, not defendant's, the daughter rarely commented on victim's Facebook page and the **style of communication** did not match that of the daughter
- The **timing** indicated that the defendant made the comments in that the daughter picked up the defendant upon his release from prison and the comments were posted shortly after
- Facebook messages occurred around the same **time** that voicemails were left on victim's phone; victim recognized defendant's voice in a threatening message

***State v. Ford*, 245 N.C. App. 510 (2016)**

In involuntary manslaughter trial involving dangerous dog, **screenshots of video and audio of a song**, both posted on **Myspace webpage (social media)**, were properly authenticated where:

- **Name of webpage** contained **defendant's nickname,** "Flex," and video depicting defendant's dog was captioned with **dog's name,** "DMX"
- Social media webpage contained distinctive **substantive content** such as **photos** of the defendant, **videos** of defendant's dog on a chain being called, and a song with lyrics denying that the victim's death was caused by defendant's dog
- A detective testified that he recognized the voice on the song as defendant's, and a neighbor testified that he heard the song coming from defendant's house

Ford cites to *United States v. Hassan,* 742 F.3d 104 (4th Cir. 2014) (**Facebook messages** properly authenticated where Facebook pages and Facebook **accounts** were tracked to defendant's mailing and email **addresses** using **IP (internet protocol) addresses)**.

***State v. Gray*, 234 N.C. App. 197 (2014)**

In robbery case, **text messages** between co-conspirators were properly authenticated where:

- **Substance** of text messages referred to location of trailer where victim was located, how many people were in the trailer, and the trailer door being open
- Officer testified that the text messages were found on defendant's cell phone (**device**) and that officer took a screenshot of them
- A **co-conspirator testified** that the screenshot accurately depicted the text messages she exchanged with the defendant

***State v. Taylor*, 178 N.C. App. 395 (2006)**

In kidnapping and murder case, **text messages** sent to and from victim's phone were properly authenticated where:

- A telecommunications employee testified that the messages were stored on the company server and accessible with access code
- The manager of cellphone store testified that he issued the victim the **cell phone (device)** with a particular phone number, and the text messages associated with that number were retrieved from the telecommunication company's server using the victim's access code

The **substance** of the text messages referred to the victim's first **name**, "Sean," as well as a 1998 Contour, which was the make of victim's car

INADEQUATE

Foundation for Digital Communication

***State v. Thompson*, 254 N.C. App. 220 (2017)**

In robbery case, Facebook messages allegedly sent between the defendant and victim referencing drug activity were properly excluded where:

- Defense attempted to use screenshot of messages as extrinsic evidence to impeach victim, but the subject of impeachment may have been collateral rather than material to the pending matter, and defense did not argue that it was material. *See State v. Hunt*, 324 N.C. 343 (1989) (extrinsic evidence of prior inconsistent statements may not be used to impeach a witness where the questions concern a collateral, rather than a material, matter)
- Defense did not attempt to lay a foundation for the text messages

Rankin v. Food Lion, 210 N.C. App. 213 (2011)

In hearing on motion for summary judgment in civil trial, printouts from internet webpages offered to show ownership of a Food Lion store were properly excluded where:

- Plaintiff failed to offer "any evidence tending to show what the documents in question were… " and failed to "make any other effort to authenticate [the] documents."

UNC SCHOOL OF GOVERNMENT

Daniel Spiegel, Assistant Professor
UNC School of Government
spiegel@sog.unc.edu

APRIL 2025
20250049