

Digital Evidence and Admissibility: Social Media, Cell Phones, Surveillance Video, and More

Daniel Spiegel

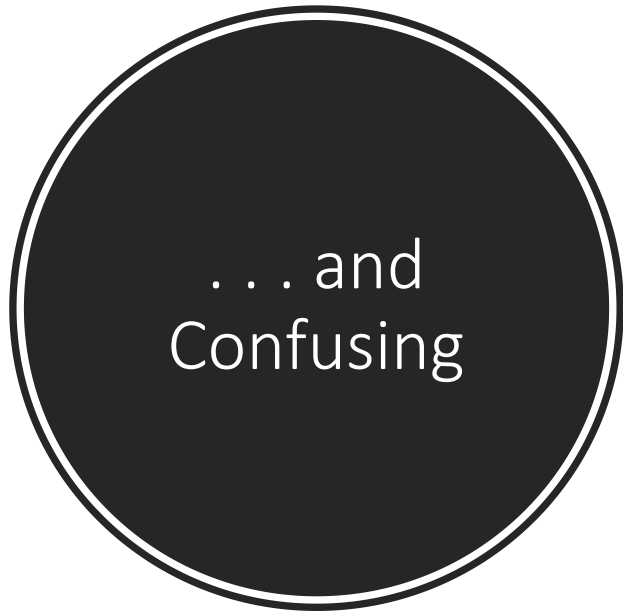
UNC School of Government

District Court Judges' Conference, June 2024

Special thanks to Jeff Welty, UNC SOG

Digital
Evidence
Can Be
Powerful






← Email Anti-spam Category

What Is Spoofing? How to Protect Yourself Against It

June 8, 2022

 by Sagar Joshi

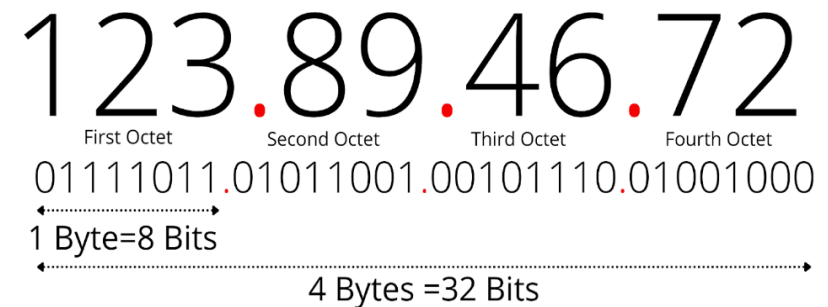
What are deepfakes – and how can you spot them?

AI-generated fake videos are becoming more common (and convincing). Here's why we should be worried

by [Ian Sample](#)



IPv4 Address Format (Dotted Decimal Notation)



The Other Side Says Your Evidence Is A Deepfake. Now What?

DECEMBER 21, 2022

PUBLICATION

*P*artner [Brent Gurney](#) and Counsel [Matthew Ferraro](#) discuss the two central concerns about deepfakes in the courtroom in an expert analysis article published by *Law360*.

Excerpt: In several recent high-profile trials, defendants have sought to cast doubt on the reliability of video evidence by suggesting that artificial intelligence may have surreptitiously altered the videos.

Related Documents

[The Other Side Says Your Evidence Is A Deepfake. Now What?](#)



Related Solutions

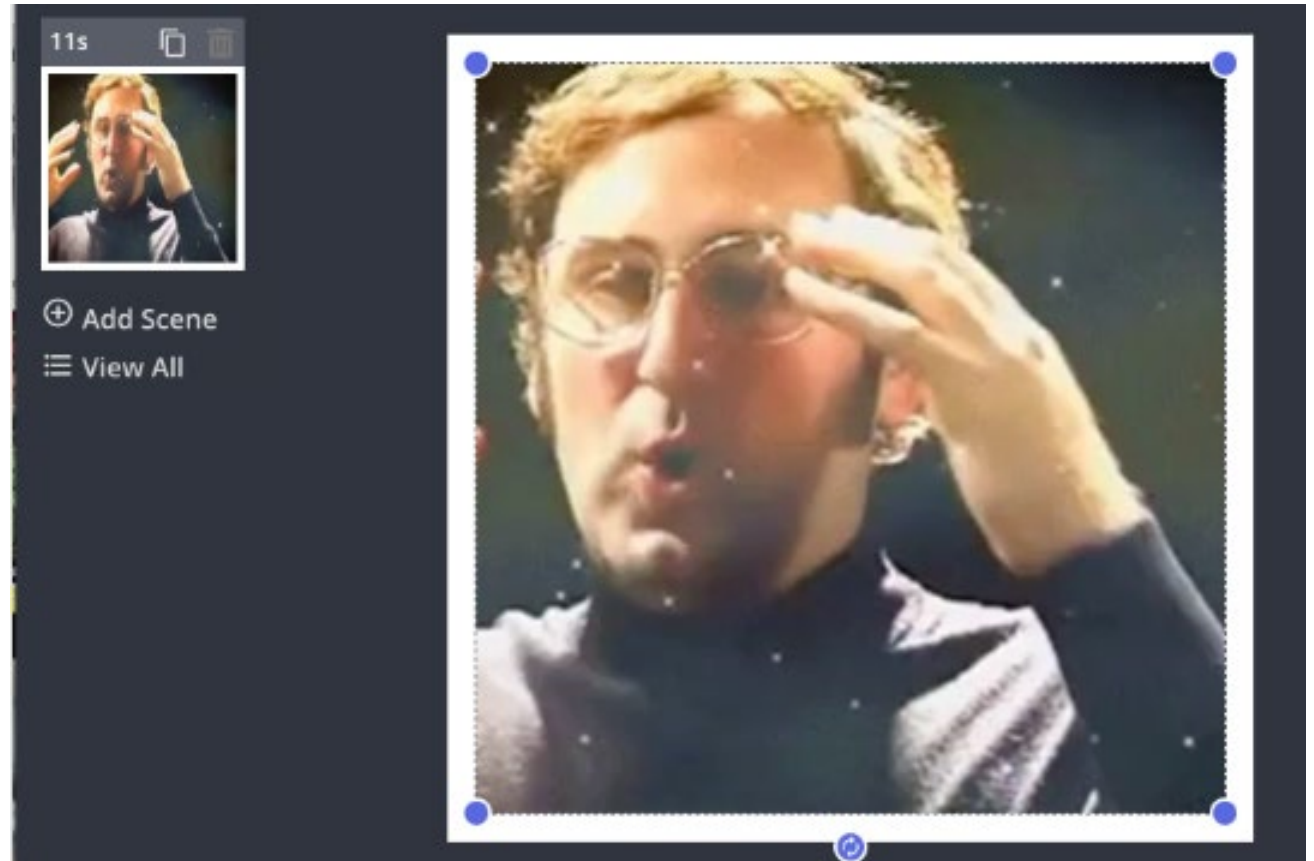
Examples from the real world - January 6th cases in federal court

- In one case, D objected to authenticity of surveillance footage from Capitol building
- In another, D crossed FBI agent on whether she was familiar with “deepfakes” (gov’t was attempting to introduce footage from D’s helmet-mounted camera)



Examples from the real world - Kyle Rittenhouse trial in Wisconsin

- Prosecutor attempted to “zoom in” on video
- Defense objected –
 - How does the technology for zooming in work?
 - Does it alter the image?



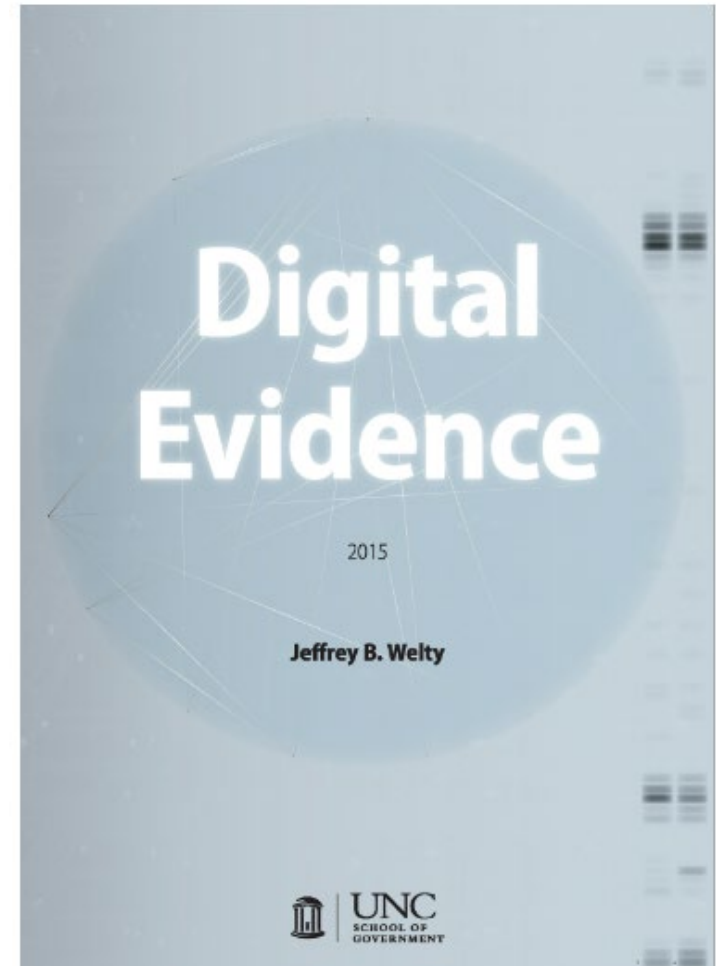
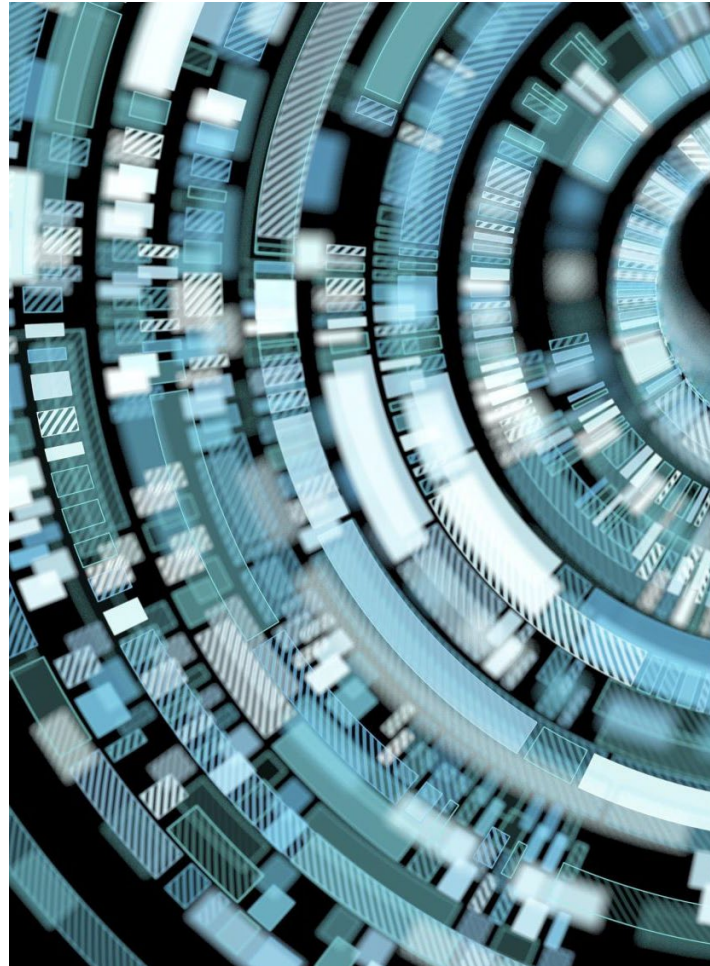
- “I don’t know if there has been, um, what would need to be done to trace this [social media post] back to a particular IP address or whatever at this time.”
 - State v. Ford, 245 N.C. App. 510 (2016)

(Stock photo, not the attorney of record)



Electronic Communications Are the Key Concern

- Everything is digital now
- But in most cases, the traditional foundation rules work well
- Communications present some special issues
- Digital Evidence Book by Jeff Welty



Is This Text Message Admissible?

- Dad and Mom break up
- He realizes he's missing \$1000 that he had set aside to pay for a medical procedure that Child needs
- Via text message, Dad accuses Mom of stealing it
- She replies, "I'm sorry, I will make it right, I took it a few months ago so I could buy you the recliner I got you for your birthday"
- He takes a screenshot of the exchange
- At a subsequent TPR proceeding, he testifies:
 - The screenshot accurately depicts the exchange
 - He received the reply from her number, which she has used for years
 - She did buy him a recliner for his most recent birthday



State v. Allen, 250 N.C. App. 823 (2016) (unpublished)

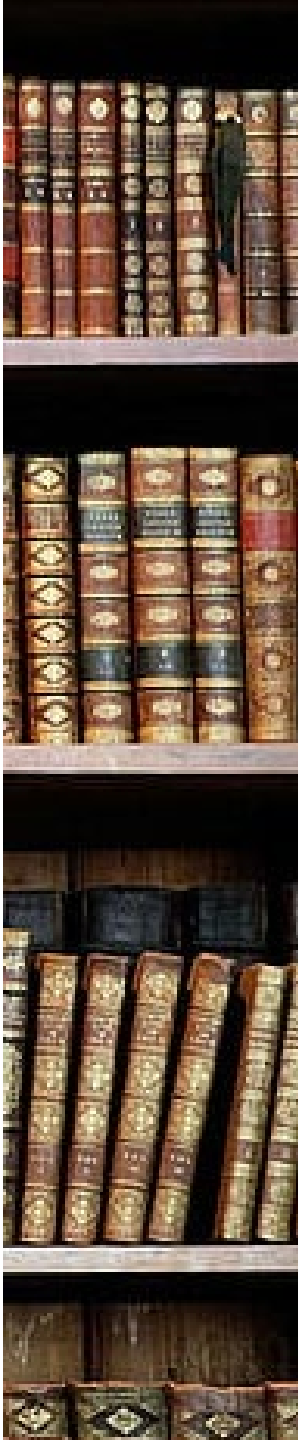
- D charged with felony larceny of \$18K in cash from her boyfriend's parents
- The boyfriend suspected her and confronted her via text message
- She responded "I'm sorry. I'm so sorry. I will make this right if it takes me 100 years."
- She referenced a gift she had given to the boyfriend
- The boyfriend forwarded the messages to a LEO, who printed them out without altering them
- The State introduced the messages through the boyfriend, who testified that he knew the messages were from D because they were from her phone number, no one else ever uses her phone, and she referenced the gift she gave him

State v. Allen, 250 N.C. App. 823 (2016) (unpublished)

- Is there a **hearsay** problem?
 - No – the messages are statements of a party opponent, Rule 801(d)
- Is there a **best evidence rule** problem?
 - No – printouts are originals under Rule 1001
- Is there an **authentication** problem?
 - No – the boyfriend is a “witness with knowledge,” Rule 901(b)(1), and the fact that the messages came from D’s phone number was a distinctive characteristic, Rule 901(b)(4)
 - There is no need to call a witness from the cell phone company to attribute the messages to D

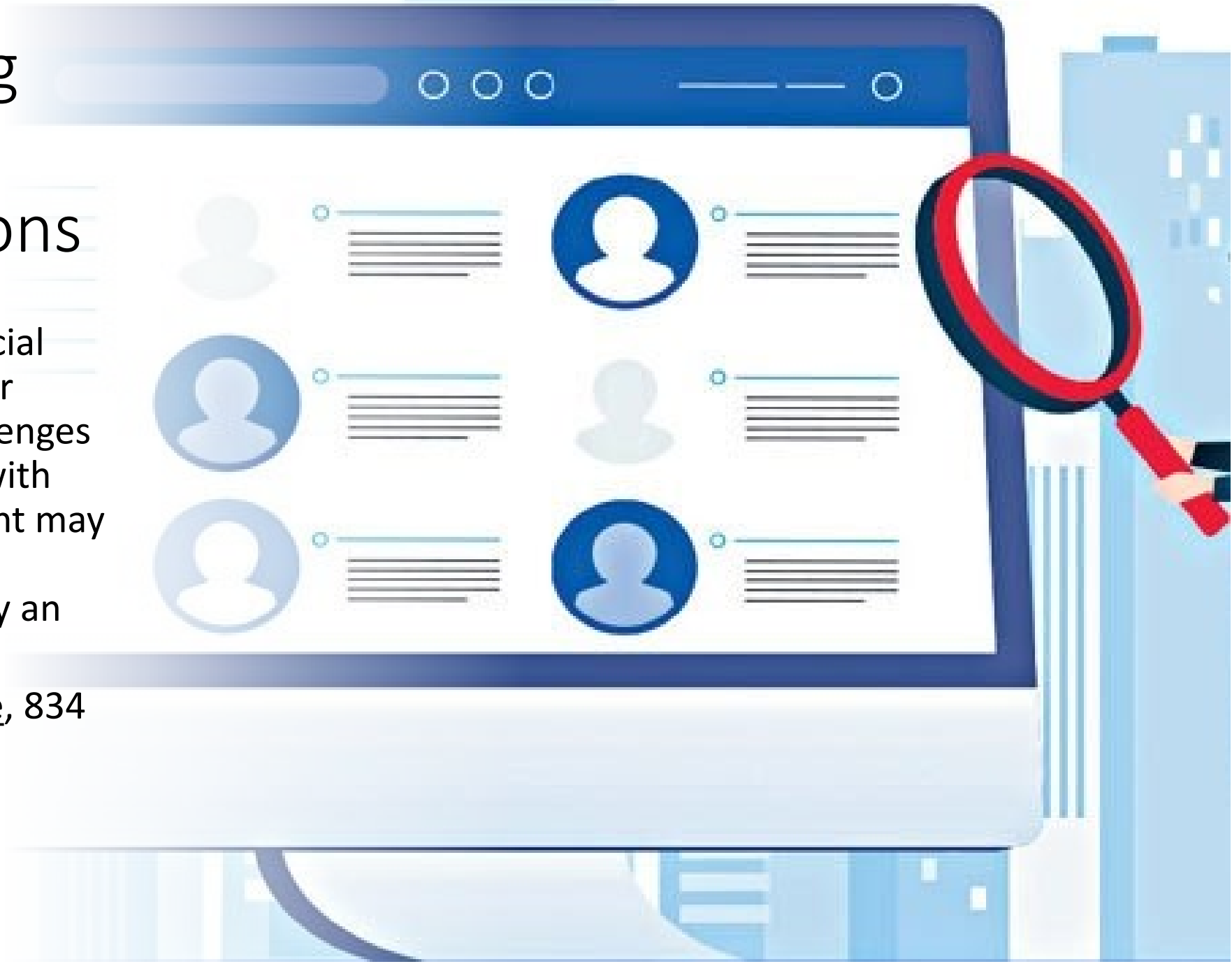
Authentication Basics

- Authentication is identification
 - The proponent must show that “the [evidence] in question is what its proponent claims.” N.C. R. Evid. 901
- Authentication is “a special aspect of relevancy”
 - Adv. Comm. Note, N.C. R. Evid. 901(a)
- Authentication is a low hurdle
 - State v. Ford, 245 N.C. App. 510 (2016) (stating that the “burden to authenticate . . . is not high – only a prima facie showing is required”)
- Authentication often comes from:
 - Testimony of a “[w]itness with [k]nowledge,” Rule 901(b)(1)
 - The “distinctive characteristics” of the evidence or other “circumstances,” Rule 901(b)(4).



Authenticating Electronic Communications

- “[T]he authentication of social media evidence in particular presents some special challenges because of the great ease with which a social media account may be falsified or a legitimate account may be accessed by an imposter.”
 - United States v. Browne, 834 F.3d 403 (3d Cir. 2016)



Two Step Authentication

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

• “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.”

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



Memory Tool: “SANDVAT”

- **“S” is for “Substance”** – how does the **substantive content of the digital evidence itself** tend to authenticate it?
 - Remember, this is appropriate under Rule 104(a)- for preliminary questions such as authenticity, the court is not bound by rules of evidence (except for privileges)
 - Example: the reference to a gift between the parties (the recliner) that only the two of them would know about
- **“A” is for “Account”** – information about the account (login, properties, pieces of identifying information associated with profile)
- **“N” is for “Name”** – is there a name or “handle” associated with the social media account?
- **“D” is for “Device”** – who possessed the phone or computer? What can we learn from the hardware itself?

Memory Tool: “SANDVAT”

- **“V” is for “Visuals”** - what do the photos/videos show on the account?
- **“A” is for “Address”** – what can we learn from the IP address or physical address associated with the evidence?
- **“T” is for “Timing”**
 - When was the post made?
 - What is the overall chronology and how does that line up with events **IRL**? (Example: the release from prison in *Clemons*)
- **“SANDVAT”** – remember, this is just a memory tool (not a legal test), but it can be a helpful way to think about the paths to authenticate digital evidence.

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

- V has a DVPO against D
- D is released from prison and their adult daughter picks him up
- Shortly thereafter:
 - V begins receiving multiple calls daily from an unknown number; the caller sometimes leaves messages referencing events from D and V's past
 - Comments appear on some of V's Facebook posts; they are made from V's daughter's account, but V testifies that her daughter never comments on her posts and wouldn't make comments of that kind
- V takes screenshots of the Facebook comments and gives them to the police, who charge D with violating the DVPO by contacting V

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

- (1) “the screenshots must have accurately reflected [V’s] Facebook page. . . . Therefore, the screenshots must have been authenticated as photographs.”
- (2) “the screenshots of the Facebook comments are also statements—the State wanted the jury to use the screenshots to conclude [D] communicated with [V] in violation of the DVPO through the Facebook comments. . . . In light of this purpose, the Facebook comments also needed to be authenticated by evidence sufficient to support finding they were communications actually made by Defendant.”

Circumstantial Evidence of Authorship

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

- D's dog DMX killed a neighbor
- D charged: involuntary manslaughter
- Did D know DMX was dangerous?
- State introduced a screenshot of what it said was D's MySpace page, featuring a video titled "DMX the Killer Pit"
- Authentic? Yes. Account name included D's nickname and account contained pictures of D and DMX



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

- Two men, including D, and two women planned to rob V
- The women met up with V and his friend at a trailer
- The women communicated with D and the other man via text messages about who was in the trailer and what was happening
- After D was arrested, a LEO searched D's phone and found the text chain, and took a screenshot
- At trial, the LEO testified about what he did and one of the women said that the screenshot showed the communication she had with D that night

Memory Tool: “SANDVAT”

- **“S” is for “Substance”** – how does the **substantive content of the digital evidence itself** tend to authenticate it?
 - Remember, this is appropriate under Rule 104(a)- for preliminary questions such as authenticity, the court is not bound by rules of evidence (except for privileges)
 - Example: the reference to a gift between the parties (the recliner) that only the two of them would know about
- **“A” is for “Account”** – information about the account (login, properties, pieces of identifying information associated with profile)
- **“N” is for “Name”** – is there a name or “handle” associated with the social media account?
- **“D” is for “Device”** – who possessed the phone or computer? What can we learn from the hardware itself?

Memory Tool: “SANDVAT”

- **“V” is for “Visuals”** - what do the photos/videos show on the account?
- **“A” is for “Address”** – what can we learn from the IP address or physical address associated with the evidence?
- **“T” is for “Timing”**
 - When was the post made?
 - What is the overall chronology and how does that line up with events **IRL**? (Example: the release from prison in *Clemons*)
- **“SANDVAT”** – remember, this is just a memory tool (not a legal test), but it can be a helpful way to think about the paths to authenticate digital evidence.



What If the Communication Is a Photo or a Video?

- United States v. Farrad, 895 F.3d 859 (6th Cir. 2018)
- D charged with being a felon in possession of a firearm
- Prosecution's sole evidence was photos taken from D's Facebook
- D: no evidence they're accurate, could be Photoshopped, don't even know when they were supposedly taken
- 6th Circuit: "not only did the details of the account match [D] . . . but . . . the photos appeared to show [D], his tattoos, and . . . distinctive features of [his] apartment . . . the photos were not . . . offered as definitive and irrebuttable proof. . . . No specific evidence was shown to suggest that the photographs were not [accurate]. . . . In short, while there were still **questions about the photos that merited probing**, those questions were not so glaring as to prevent the photos from clearing the relatively lower hurdle of authentication."

What If the Evidence Comes from a Technology Company?

- United States v. Recio, 884 F.3d 230 (4th Cir. 2018)
- D charged with unlawful gun possession
- Prosecution offered a Facebook post quoting a rap lyric about always carrying a gun
- Authentic?
- 4th Circuit:
 - Step one (accuracy): Facebook (the custodian) certified the posting as a business record
 - Step two (authorship): username and email address associated with the account contained D's name and the account contained photos of D and birthday wishes to D

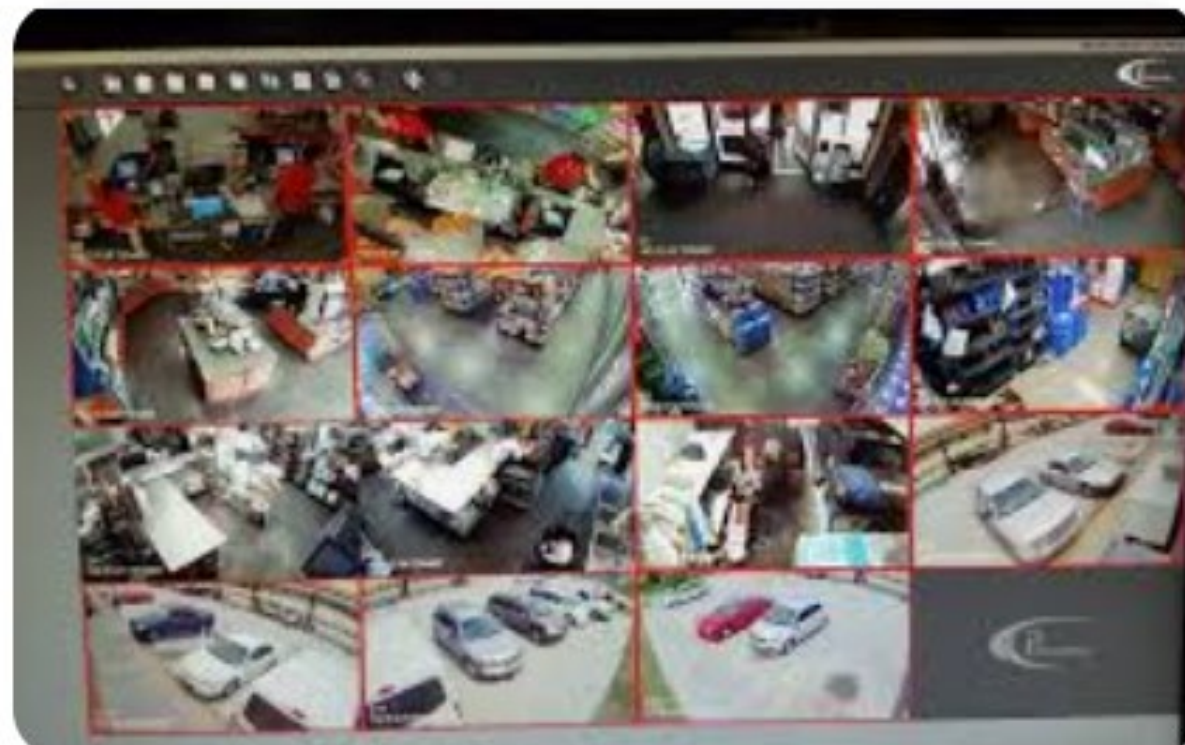


Surveillance Video



Authenticating Surveillance Video

- **Fair and Accurate** method (Illustrative)
 - Witness was present during the recorded events and can testify that the footage is a “fair and accurate” depiction of what occurred
 - Ex. Loss Prevention Officer was actually there and saw D steal items at the store
- **Silent Witness** method (Substantive)
 - No live witness
 - Footage has been retrieved and there is either a chain of custody for the footage or some other combination of factors that go to authenticity/reliability



State v. Jones

North Carolina Criminal Law

A UNC School of Government Blog

Home

Surveillance Video- When It Comes In and When It Doesn't

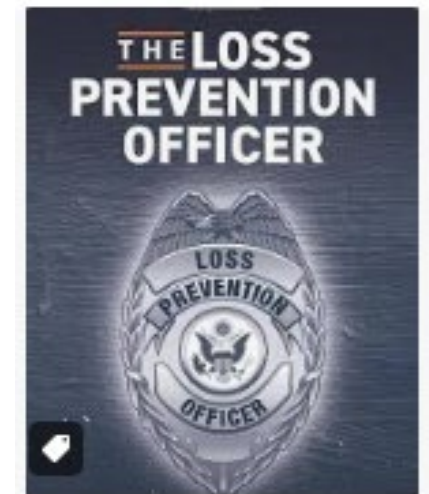
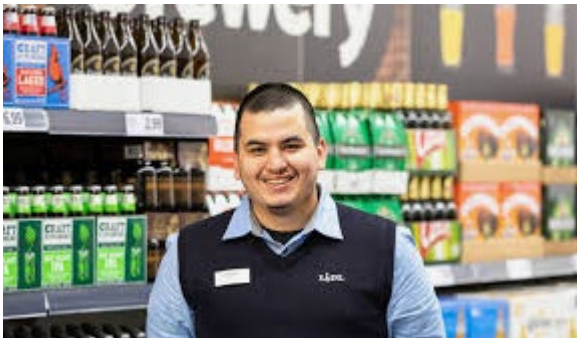
March 25, 2024 [Daniel Spiegel](#)

Print

Video evidence authentication has received a [fair amount of treatment](#) on this blog. The topic remains an area of practical significance given the prevalence of video evidence in criminal trials and how common it is for the prosecution's case to hinge on the admission of video. We are increasingly a [video-focused](#) society. Between home security cam, doorbell cam, body-worn cam, in-car cam, pole cam, and even [parking lot cam](#), juries increasingly expect to see video, whether the incident in question occurred outside a home, near a business, or on the roadside.

Surveillance Video- Common Authenticating Witnesses

- Loss Prevention Officer
- Store Clerk
- Store Manager
- Homeowner
- Law Enforcement Officer who extracted the video from the system (may or may not be specialist/expert)
- Investigating Officer (think *State v. Jones*)



State v. Jones

ADEQUATE

Foundation for Surveillance Video*

State v. Jones, 288 N.C. App. 175 (2023)

Officer testified that:

1. Video was same as footage she saw on night of incident;
 2. Homeowner's description of events matched the video;
 3. Surveillance system was working correctly "to [her] knowledge."
-

State v. Snead, 368 N.C. 811 (2016)

Loss prevention manager testified that:

1. He was familiar with recording equipment and it was in working order;
 2. He viewed the footage on the recording equipment and video was same as the footage he viewed.
-

State v. Fleming, 247 N.C. App. 812 (2016)

Corporate investigator testified that:

1. He was familiar with the recording system, it was functioning properly, and he made a copy of footage;
 2. Video was the same as footage he copied, unedited, and same as that created by system.
-

State v. Ross, 249 N.C. App. 672 (2016)

Store manager testified that:

1. Cameras were working properly because time and date stamps were accurate;

INADEQUATE

Foundation for Surveillance Video*

State v. Moore, 254 N.C. App. 544 (2017)

Officer testified that:

1. The day after the incident, since store manager was unable to make a copy of the footage, officer recorded footage on the store's equipment with his cell phone;
2. The video, which was a copy of the cell phone recording, accurately showed footage he had reviewed at the store.

Store clerk testified that the defendant was seen on video, but did not testify as to whether the video accurately depicted events he observed on day in question.

No testimony pertaining to type of recording equipment and whether it was in good working order/reliable.

State v. Mason, 144 N.C. App. 20 (2001)

Two store employees testified that surveillance system was in working order but were unfamiliar with maintenance, testing, or operation.

State v. Jones

ADEQUATE

Foundation for Surveillance Video*

***State v. Jones*, 288 N.C. App. 175 (2023)**

Officer testified that:

1. Video was same as footage she saw on night of incident;
2. Homeowner's description of events matched the video;
3. Surveillance system was working correctly "to [her] knowledge."

State v. Moore

INADEQUATE

Foundation for Surveillance Video*

***State v. Moore*, 254 N.C. App. 544
(2017)**

Officer testified that:

1. The day after the incident, since store manager was unable to make a copy of the footage, officer recorded footage on the store's equipment with his cell phone;
2. The video, which was a copy of the cell phone recording, accurately showed footage he had reviewed at the store.

State v. Moore (continued)

Store clerk testified that the defendant was seen on video, but did not testify as to whether the video accurately depicted events he observed on day in question.

No testimony pertaining to type of recording equipment and whether it was in good working order/reliable.

Surveillance Video- Example

- Misdemeanor Larceny trial
- Loss Prevention Officer (LPO) from Walmart is present
 - The LPO retrieved the disc from where it was stored at the store
 - The LPO was not present during the incident
 - A previous LPO (who quit) was the one who burned the disc from the system
- Would you admit the surveillance video? Why?

Mechanics of Receiving Digital Evidence in District Court

- What happens when moving party tries to get in evidence directly off the phone?
- From General Rules of Practice for the Superior and District Courts:

Rule 14. Custody and Disposition of Evidence at Trial

Once any item of evidence has been introduced, the clerk (not the court reporter) is the official custodian thereof and is responsible for its safekeeping and availability for use as needed at all adjourned sessions of the court and for appeal.

After being marked for identification, all exhibits offered or admitted in evidence in any cause shall be placed in the custody of the clerk, unless otherwise ordered by the court.

- Should video evidence be burned onto a new disc? (Initials and date on copy)
- Using Printouts as exhibits



Questions

Digital Evidence and Admissibility: Social Media, Cell Phones, Surveillance Video, and More

Daniel Spiegel

UNC School of Government

District Court Judges' Conference, June 2024

Special thanks to Jeff Welty, UNC SOG

When is an expert necessary?

Or at least a records custodian?

- **Cell Site Location Information**

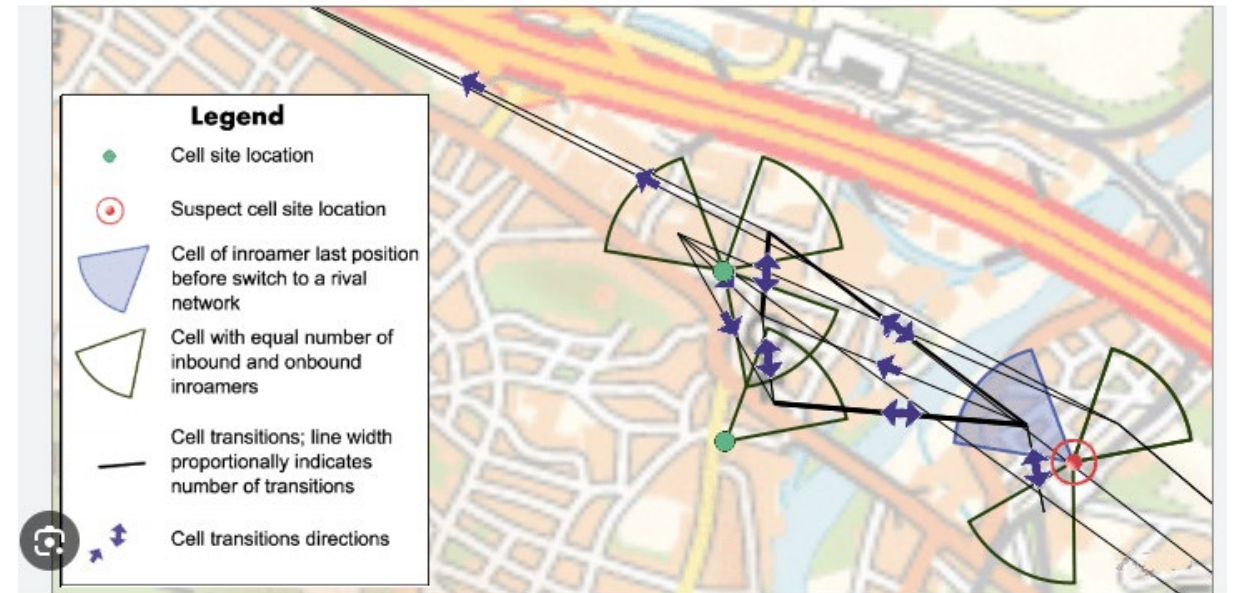
- Expert likely necessary
- Complex technology and methodology involved -sectors, pings
- Often FBI involvement or other specialist

- **“Find my phone” location info?**

- **Social media posts?**

- **Emails?**

- **Texts?**



When is an expert necessary? Or at least a records custodian?

Rule 803(6): Please Hold for the Next Available Representative...



March 13, 2018 [Jonathan Holbrook](#)

Print

A few weeks ago I participated in a seminar on digital evidence, and one of the topics we discussed was cell phone records (subscriber information, call detail records, historical location data, etc.). That's not surprising, since the widespread use of cell phones has made these records an increasingly common and important tool in criminal cases. Location data can help prove that the defendant was in the victim's house at the time of the murder, call logs can help prove the co-conspirators were in regular contact with each other, and so on.

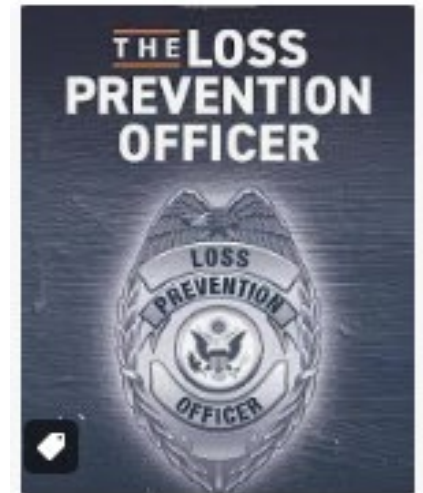
What did surprise me was when I asked a group of 75+ prosecutors how often they have used an affidavit to authenticate these kinds of records and get them

Does records custodian need to be present?

- **Recent change to Rule 803(6) last year – S.L. 2023-151**
 - **Allows unsworn declaration “under penalty of perjury” instead of notarized affidavit to authenticate a business record without live appearance of records custodian**
- **Notice requirement:**
 - **“advance notice” required**
 - **unclear exactly what is reasonable for time frame**

Surveillance Video- (side issue- can witness NARRATE video?)

- *State v. Patterson*, 249 N.C. App. 659 (2016)
- *State v. Belk*, 201 N.C. App. 412 (2009)
- Lay opinion – general rule:
 - Admissible if helpful to fact finder and doesn't invade province of jury
- Factors:
 - Witness familiar with D's appearance
 - Witness familiar with D's appearance on offense date or at a time when D dressed like they dressed on offense date
 - Whether D disguised or altered appearance



Surveillance Video- (side issue- Time Stamp battles)

- What if time stamp is “pretty close?”
- What if time stamp is off by an exact number of hours?
- Does this affect admissibility of entire exhibit or is this just a line of questioning on cross?

