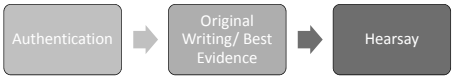
Authentication of Digital Evidence

Jeff Welty
UNC School of Government

Analytic Framework for Digital Evidence



Authentication: The Principal Issue

"[T]he novel question regarding the admissibility of web-based evidence . . . is going to be authentication. . . . [M]ost of the rest of the evidentiary problems are the common problems lawyers face all the time."

- G. Michael Fenner, The Admissibility of Web-Based Evidence, 47 Creighton L. Rev. 63 (2013)

Authentication: Split of Authority

"The . . . authentication rule[s] . . . require a demonstration that a piece of evidence is what its proponent claims it to be. But the generality of this rule has sent courts off in different directions, with some courts more skeptical of the origins of digital communications in light of the ease with which people can create accounts."

- Hugh Kaplan, Two State Courts Provide Guidance on Authenticating Texts, Facebook Messages, Bloomberg BNA Criminal Law Reporter, April 24, 2015

Authentication Basics

- Authentication is identification
  - N.C. R. Evid. 901(a) ("The requirement of authentication or identification . . . is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.")
- Authentication is "a special aspect of relevancy"
  - Adv. Comm. Note, N.C. R. Evid. 901(a)
- Authentication is a low hurdle

Methods of Authentication

- Rule 901(b) gives examples:

  (1) Testimony of a witness with knowledge. – Testimony that a matter is what it is claimed to be.

  (4) Distinctive characteristics and the like. – Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

  (7) Public records or reports. – Evidence that a writing . . . is from the public office where items of this nature are kept.
- Rule 902 lists self-authenticating evidence

Types of Digital Evidence

- Electronic communications
  - Email
  - Text messages
  - Social media posts
- Tracking data
- Data seized from a device
- Web pages

Authentication: Communications

- Testimony of a witness with knowledge
- Distinctive characteristics
  - Name or "signature" alone normally is not enough to authenticate
  - Ownership of originating account is significant support for authentication
  - Other circumstantial evidence may be needed

Authenticating Communications: Problem 1

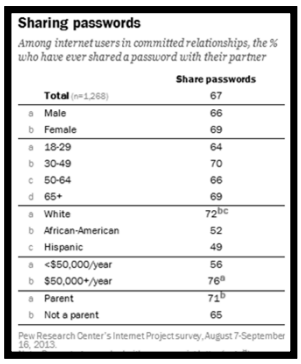
The defendant is charged with cyberstalking a neighbor because of a land dispute. The state seeks to introduce an email from the defendant to a friend who helped with the harassment of the victims. The friend is testifying for the State and is prepared to say that he received the email from the defendant's account, which the defendant had used for years; that the email was signed with the defendant's "typical signature"; and that it referenced the harassment scheme.

Authenticating Communications: Problem 2

The defendant is charged with kidnapping. The prosecution contends that he restrained his girlfriend in his home and beat her because he suspected her of infidelity. A week before trial began, she received threatening text messages referencing her "snitching" and saying things like "I'll kill u myself." She is prepared to testify about the messages; to state that the number from which they came belongs to the defendant; and to state that the defendant "called in between the [text message] conversations talking mess."

Authenticating Communications: Problem 3

The defendant is charged with assault. He went to pick up his girlfriend at a party and got in a fight with another woman. He claims self-defense. The woman is testifying, and defense counsel wishes to cross-examine her with printouts from her Facebook account that suggesting animosity towards the defendant's girlfriend ("ima f*** that . . . b**** up") and the defendant ("her bf is a dead man walkn"). The victim acknowledges that the statements came from her account but testifies that she has shared her user name and password with others; that her account has been hacked before; and that she does not remember writing some of the statements at issue.



Sharing passwords

Among internet users in committed relationships, the % who have ever shared a password with their partner

		Share passwords
	Total (n=1,268)	67
a	Male	66
b	Female	69
a	18-29	64
b	30-49	70
c	50-64	66
d	65+	69
a	White	72[bc]
b	African-American	52
c	Hispanic	49
a	<$50,000/year	56
b	$50,000+/year	76[a]
a	Parent	71[b]
b	Not a parent	65

Pew Research Center's Internet Project survey, August 7-September 16, 2013

Factors in Authenticating Electronic Communications

- Purported author acknowledges authorship of communication
- Purported author acknowledges ownership of account
- Account name contains purported author's name
- Account profile contains picture of purported author
- Account profile contains identifying data associated with purported author (DOB, physical address, etc.)
- Account has been used by purported author in the past
- Purported author has had exclusive control of account in the past
- Account was created on purported author's device or from purported author's home
- Account normally accessed on purported author's device or from purported author's home
- When the communication was sent, account was accessed on purported author's device or from purported author's home
- Communication contains words, phrases, or signature characteristic of purported author
- Communication concerns events only known to, or of special interest to, purported author
- Communication is connected in time or content to other communications clearly written by purported author
- Timing of communication connects to events in life of purported author

Authenticating Communications: Problem 4

Defendant is charged with assault and attempted murder after stabbing his ex-girlfriend. He claims self-defense. She is prepared to testify that, shortly after the stabbing, the defendant sent her a Facebook direct message asking her to forgive him and stating that he "got carried away by the anger." She has a screenshot of the message. She also has a handwritten note that she received shortly thereafter expressing similar sentiments, which she says is also from him.

Authentication: Tracking Data

Location data is commonly introduced in criminal cases

- Data collected through surreptitious GPS tracking, e.g., from a device an officer installs on a suspect's car
- Data collected through GPS monitoring of sex offenders
- Data collected through GPS monitoring of defendants on pretrial release
- GPS or cellular tower data obtained from a suspect's cellular telephone service provider

Authentication Rules for Tracking Data

- Rule 901(b)(1): Testimony of a witness with knowledge
- Rule 901(b)(9): "Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result"

Authenticating Tracking Data: Problem 1

The defendant is charged with sexually assaulting a woman. At the time of the assault, he was wearing a GPS monitoring device as a condition of his pretrial release on another charge. The officer who heads the pretrial release electronic monitoring unit is prepared to testify to the defendant's whereabouts on the night in question and to plot the defendant's location on a map. He has been trained by the manufacturer of the monitoring device and has several years of experience with its use, but he isn't an expert on how GPS works.

Authenticating Tracking Data: Problem 2

The defendant is charged with trafficking in cocaine. The State plans to call an SBI agent as an expert in cellular analysis to trace the defendant's movements -- from a pickup location to a stash house to a meeting with a buyer -- based on the towers and faces to which the defendant's phone connected. The agent can explain how he obtained the information from the service provider, but the State does not plan to call any employees of the service provider. The agent has been trained in cell site tracking but does not have a relevant academic degree or work experience in telecommunications.

Authentication: Seized from Device

Usually authenticated by testimony about retrieval and retention

- "[T]he government properly authenticated the videos and images [of child pornography] under Rule 901 by presenting detailed evidence as to the chain of custody, specifically how the images were retrieved from the defendant's computers."
  - United States v. Salcido, 506 F.3d 729 (9th Cir. 2007)
- "Because the objects at issue here—the [child pornography] images found on defendant's computer devices—are a direct part of the charges against defendant, they are properly characterized as real evidence. To authenticate real evidence, the proponent need only establish a chain of custody,"
  - People v. Brown, 313 P.3d 608 (Colo. Ct. App. 2011)

Seized from Device: Problem 1

The defendant is charged with assaulting his ex-wife. The State seeks to admit sexually suggestive images and text messages that it contends were exchanged between the ex-wife and a boyfriend. An officer recovered the images and messages from the defendant's cellular telephone. The ex-wife remembers sending some of them, but nor others. The State seeks to introduce all of the material as evidence of the defendant's motive for the assault.

Seized from Device: Problem 2

In a child pornography case, a detective is prepared to testify that he followed sound forensic practices in recovering certain images from the defendant's computer, which he then accurately printed out. The defendant contends that the images are not properly authenticated absent a showing that they depict real children as opposed to computer-generated ones.

Seized from Device: Problem 3

The defendant is charged with sexually assaulting a friend's daughter during an overnight visit to the friend's home. The State contends that the defendant spent the night accessing pornography on the friend's computer and assaulted the child shortly thereafter. The friend is prepared to testify that the day after the assault, he checked his computer's browser history and found a list of pornographic websites that were visited during the night in question, with the specific times that they were visited. He pasted the list into a word processing document.

Authentication: Web Pages

Many types of pages might be offered

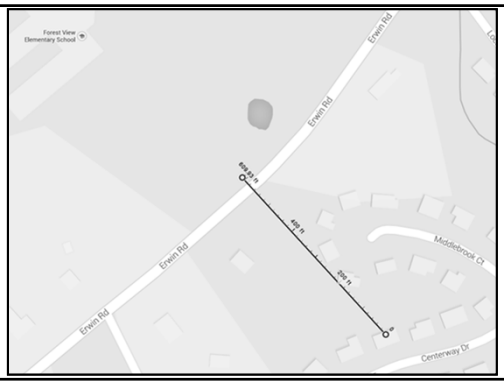
- Government websites
- Websites associated with a party
  - Including superseded or archived versions
- Mapping websites

Authenticating Web Pages: Problem 1

The defendant is charged with promoting prostitution. An investigating officer has a printout of ifshewontiwill.com, which he claims is the defendant's website. The printout contains the photographs of several women and a list of sexual services offered by each. The officer seized a business card from the defendant's house that contained the defendant's name and the address of the website.

Authenticating Web Pages: Problem 2

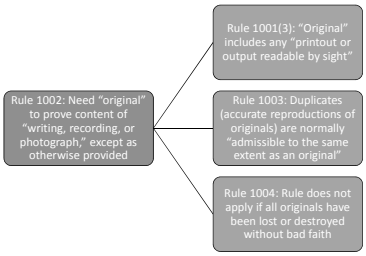
The defendant is charged with PWISD cocaine within 1000 feet of a school. The investigating officer has a printout of a Google Map, which she is prepared to testify fairly and accurately depicts the relevant area. She has not measured the area herself, but the map includes a line, generated by Google Maps, showing that the distance from the point of arrest to the school is 609.93 feet.



Authenticating Web Pages: Problem 3

The defendant is charged with armed robbery. The investigating officer downloaded a music video from YouTube that appears to show the defendant holding a gun. The State seeks to introduce the video to show that the defendant had access to a firearm. The video is undated but the defendant appears to be approximately the same age that he was at the time of the robbery.

Original Writing/Best Evidence Rule



Original Writing Rule: Problem 1

In a statutory rape case, the victim's mother is prepared to testify that a month before the alleged rape, she was logged into the victim's Facebook account, inspecting its contents. While she was doing so, a message arrived from the defendant via Facebook's on-line chat feature. The message appeared next to the defendant's picture and name stating: "Hey. Can't stop thinking about u!" The mother isn't an advanced Facebook user and didn't save the message. The defendant's lawyer says that the defendant's 13-year-old brother uses the defendant's Facebook account and knows the victim. Is the victim's mother's testimony admissible?

Hearsay

- Common hearsay exceptions in digital evidence cases
  - Admission of a party opponent
  - Business records
  - Non-hearsay

Hearsay: Problem 1

In a burglary case, the State contends that one of the defendants was acting as a lookout while the other went inside the home. The alleged lookout claims that he wasn't involved at all and was just in the wrong place at the wrong time. An officer obtained the lookout's cell phone records, which show that he called the inside guy just as the police arrived. How can the State introduce the records?