PROGRAM MATERIALS
Program #32245
December 15, 2022

Admissibility and Use of Digital Evidence at Trial

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Admissibility and Use of Digital Evidence at Trial

Brian M. Chase, Esq.
Managing Director
Digital Forensics and eDiscovery

BChase@ArcherHall.com
855.839.9084

ARCHERHALL
AIM HIGH

ARCHERHALL
AIM HIGH

Digital Forensics & eDiscovery experts serving attorneys in all 50 states

- Cellphones
- Computers & Tablets
- External Hard Drives
- Smart Devices
- Emails & SMS
- Social Media Accounts
- Cloud Data
- Electronic Medical Records

Business Litigation

Employment Law

Schools and Higher-Ed

Medical Malpractice

IP Theft

Bankruptcy

About Brian Chase

- Undergraduate Degree in MIS from the University of Arizona
- Law Degree from the University of Arizona
- Licensed to practice law in Arizona and New York
- Director of Digital Forensics at ArcherHall
- Adjunct Professor of Law at the University of Arizona
- Numerous digital forensics certifications
- Testimony in State and Federal Court, Civil and Criminal Cases
- Misdemeanor and Felony trials as an attorney

Rule 901

ARCHERHALL
AIM HIGH

Rule 901 – Authenticating or Identifying Evidence

In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

Rule 901

United States v. Vidack, 553 F.3d 344 (4th Cir. 2009)

- "[T]he burden to authenticate under Rule 901 is not high—only a prima facie showing is required," and a "district court's role is to serve as gatekeeper in assessing whether the proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic."

Rule 902 – Evidence That is Self-Authenticating

1-5:	• Public Documents
6:	• Newspapers and Periodicals
7:	• Trade Inscriptions
8:	• Acknowledged Documents
9:	• Commercial Paper
10:	• Presumptions Under a Federal Statute
11-12:	• Certified Records of a Regularly Conducted Activity
13:	• Certified Records Generated by an Electronic Process or System
14:	• Certified Data Copied from an Electronic Device, Storage Medium, or File

Rule 902 – Evidence That is Self-Authenticating

(13) Certified Records Generated by an Electronic Process or System.

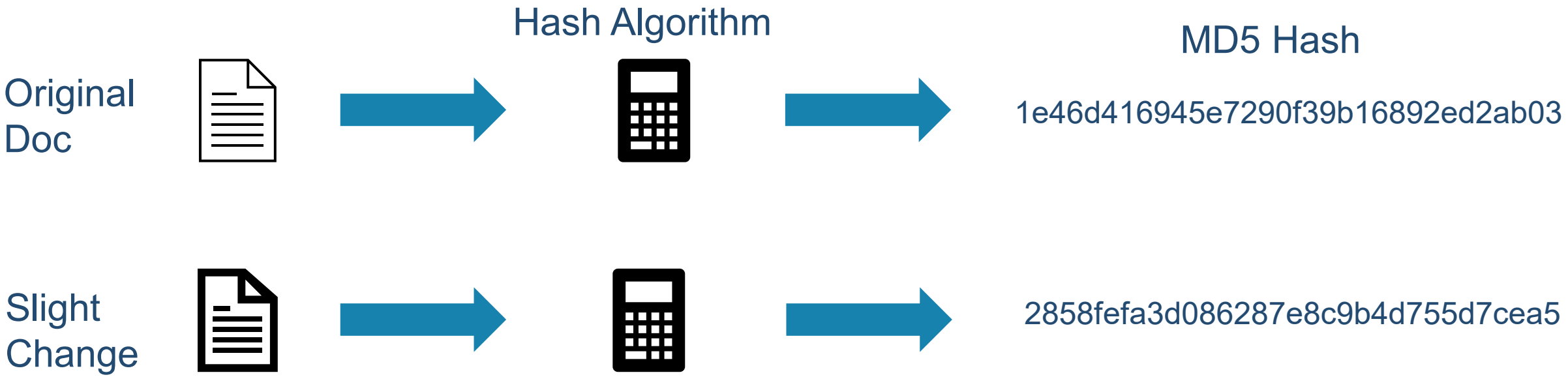
- A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

(14) Certified Data Copied from an Electronic Device, Storage Medium, or File.

- Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule (902(11) or (12). The proponent also must meet the notice requirements of Rule 902 (11).

902(14) – Hash Values

- "A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures." –Microsoft



902(14) – United States v. Dunnican

- ATF Agent Snyder certified the following: (1) that he extracted data from Dunnican's cellular telephone on March 25, 2018 through the use of specialized forensic software, which created an accurate and reliable duplication of the data; and (2) that the forensic software generated a "digital fingerprint" (otherwise known as a "hash"), which indicated that the extraction was successful, complete, and accurate.

- "In compliance with Rules 902(11) and 902(14), the government filed a notice of its intent to use a certification method on September 17, 2018. This certification was signed by ATF Special Agent Joshua Snyder, who performed the digital extraction … we conclude that the district court did not commit plain error in admitting it."

  United States v. Dunnican, No. 19-3092, 2020 WL 3056229, at *7 (6th Cir. June 9, 2020)

Hearsay

ARCHERHALL
AIM HIGH

Rules 801 and 802

Rule 801

- (a) Statement. “Statement” means a person’s oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion.
- (b) Declarant. “Declarant” means the person who made the statement.
- (c) Hearsay. “Hearsay” means a statement that:
  - (1) the declarant does not make while testifying at the current trial or hearing; and
  - (2) a party offers in evidence to prove the truth of the matter asserted in the statement.

Rule 802

- Hearsay is not admissible unless any of the following provides otherwise:
  - a federal statute;
  - these rules; or
  - other rules prescribed by the Supreme Court.

801(d)(2) – Party Opponent

- **801(d)(2) An Opposing Party's Statement. The statement is offered against an opposing party and:**
  - (A) was made by the party in an individual or representative capacity;
  - (B) is one the party manifested that it adopted or believed to be true;
  - (C) was made by a person whom the party authorized to make a statement on the subject;
  - (D) was made by the party's agent or employee on a matter within the scope of that relationship and while it existed; or

803(6) – "Business Records"

(6) *Records of a Regularly Conducted Activity*. A record of an act, event, condition, opinion, or diagnosis if:

- **(A)** the record was made at or near the time by — or from information transmitted by — someone with knowledge;
- **(B)** the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
- **(C)** making the record was a regular practice of that activity;
- **(D)** all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and

803(6) – "Business Records"

United States v. Daneshvar, 925 F.3d 766, 777 (6th Cir. 2019)

- An email is not a business record for purposes of the relevant hearsay exception simply because it was sent between two employees in a company or because employees regularly conduct business through emails; such evidence alone is insufficient to show that the email is a record, made as "a regular practice" of the company

United States v. Cone, 714 F.3d 197, 220 (4th Cir. 2013)

- "[I]t would be insufficient to survive a hearsay challenge simply to say that since a business keeps and receives e-mails, then *ergo* all those e-mails are business records falling with the ambit of Rule 803(6)(B).

US v. Ayelotan, 917 F.3d 394 (5th Cir. 2019)

- District court admitted emails produced by Google and Yahoo! purporting to be from the Defendants
- Email records included certificates saying the data was recorded as part of regularly conducted business activity
- Court rules that the certificate made the document self-authenticating and admissible under 803(6)
- Court ruled the content within the email was admissible under 801(d) as it was statements from the defendant and statements in furtherance of the conspiracy

- Court did not address foundation requirements to establish that the email accounts actually belong to, and were used by, the defendant.

Expert Witnesses
Rule 701-703

ArcherHall
AIM HIGH

Rule 701. Opinion Testimony by Lay Witnesses

If a witness is not testifying as an expert, testimony in the form of an opinion is limited to one that is:

- **(a)** rationally based on the witness's perception;
- **(b)** helpful to clearly understanding the witness's testimony or to determining a fact in issue; and
- **(c)** not based on scientific, technical, or other specialized knowledge within the scope of Rule 702.

Rule 702. Testimony by Expert Witnesses

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

- **(a)** the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
- **(b)** the testimony is based on sufficient facts or data;
- **(c)** the testimony is the product of reliable principles and methods; and
- **(d)** the expert has reliably applied the principles and methods to the facts of the case.

Rule 703. Bases of an Expert

An expert may base an opinion on facts or data in the case that the expert has been made aware of or personally observed. If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. But if the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.

Best Evidence Rule 1001

ARCHERHALL
AIM HIGH

Best Evidence

Rule 1002 - Requirement of the Original

- An original writing, recording, photograph, or video is required in order to prove its content unless these rules or an applicable statute provides otherwise.

Rule 1003. Admissibility of Duplicates

- A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate.

Some Cases

ARCHERHALL
AIM HIGH

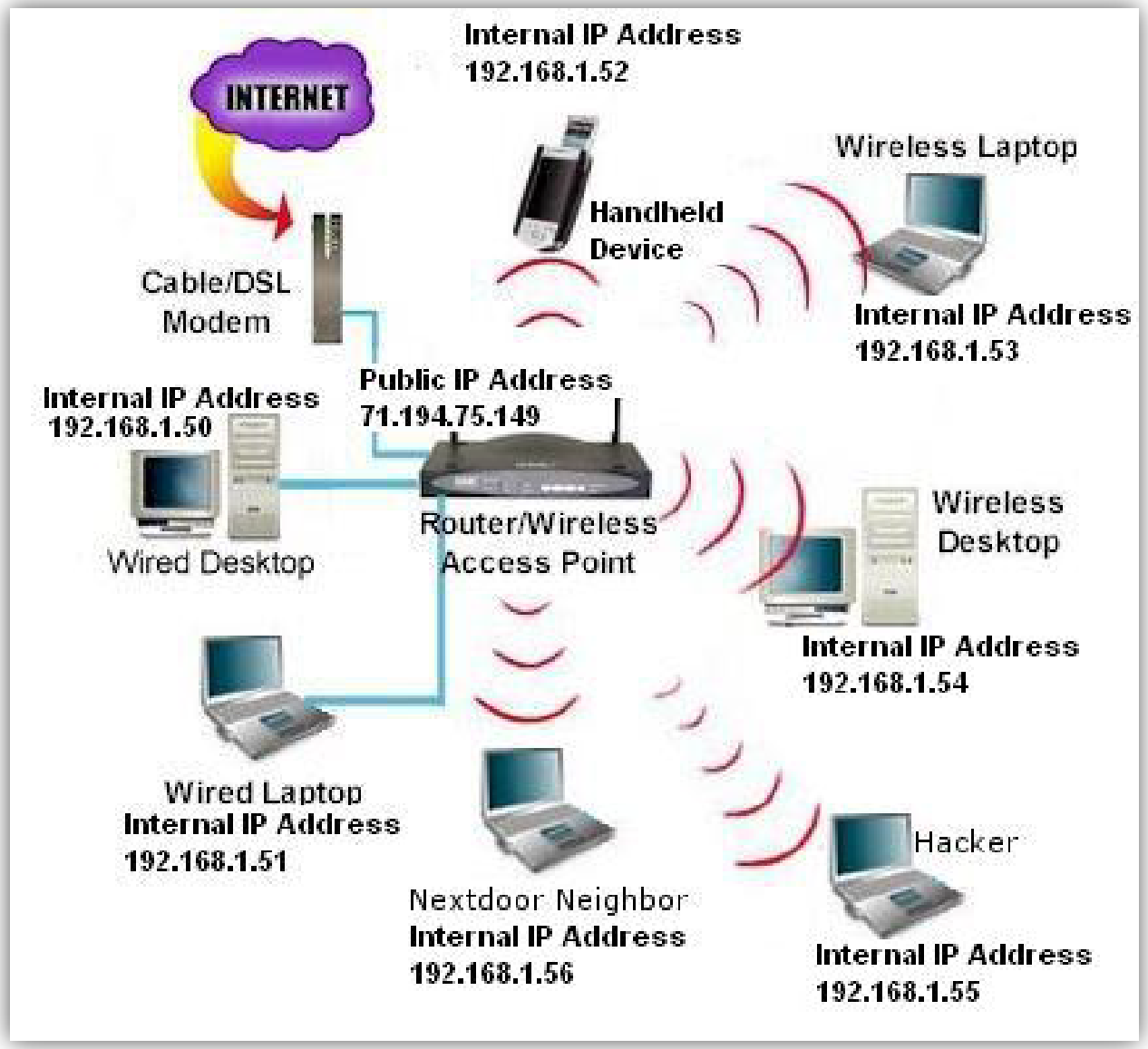
Facebook and YouTube Page

- Screenshots of the defendant's Facebook and YouTube Page
- Facebook screenshots showed the defendant's biographical information, with listing of their interests
- Facebook page had links to the YouTube Page
- Certification from custodian of records for Facebook and Google, verifying that the pages had been maintained in the regular course of business
- Finally, tying the accounts to the defendant via IP Address

- Ruling: Admissible.

"In these circumstances, there was no abuse of discretion in the admissions of any of the Facebook pages and YouTube videos." *U.S. v. Hassan*, 742 F.3d 104, 133-34

IP Address


INTERNET
Internal IP Address
192.168.1.52
Handheld
Device
Wireless Laptop
Internal IP Address
192.168.1.53
Cable/DSL
Modem
Public IP Address
71.194.75.149
Internal IP Address
192.168.1.50
Wired Desktop
Router/Wireless
Access Point
Wireless
Desktop
Internal IP Address
192.168.1.54
Wired Laptop
Internal IP Address
192.168.1.51
Nextdoor Neighbor
Internal IP Address
192.168.1.56
Hacker
Internal IP Address
192.168.1.55

Website Printout

- Printout of a website
- Witness has not previously seen the printout or website
- From the American Board of Emergency Medicine ("ABEM")
- Witness agrees ABEM is an authoritative/trusted organization
- Website only used on cross

- Ruling: Not admissible
  "Here, the trial justice did not make any comments or findings with respect to authentication of any of the documents in overruling plaintiff's objections to the exhibits. It is our considered opinion that insufficient evidence was proffered to support the authenticity of the two printouts of the ABEM web page."
  O'Connor v. Newport Hosp., 111 A.3d 317, 324 (R.I. 2015)

Websites

To authenticate a printout of a web page, the proponent must offer evidence that:

- the printout accurately reflects the computer image of the web page as of a specified date;
- the website where the posting appears is owned or controlled by a particular person or entity; and
- the authorship of the web posting is reasonably attributable to that person or entity.

Christopher B. Mueller and Laird C. Kirkpatrick, 5 *Federal Evidence* § 9:9 (4th ed.)

Websites

- Printout of a website after a terrorist attack
- Relied on by an expert to say an individual acted on behalf of an organization
- Organization claimed credit for the actions of the individual
- Expert testifies that scholars, journalists, and law enforcement rely on the website

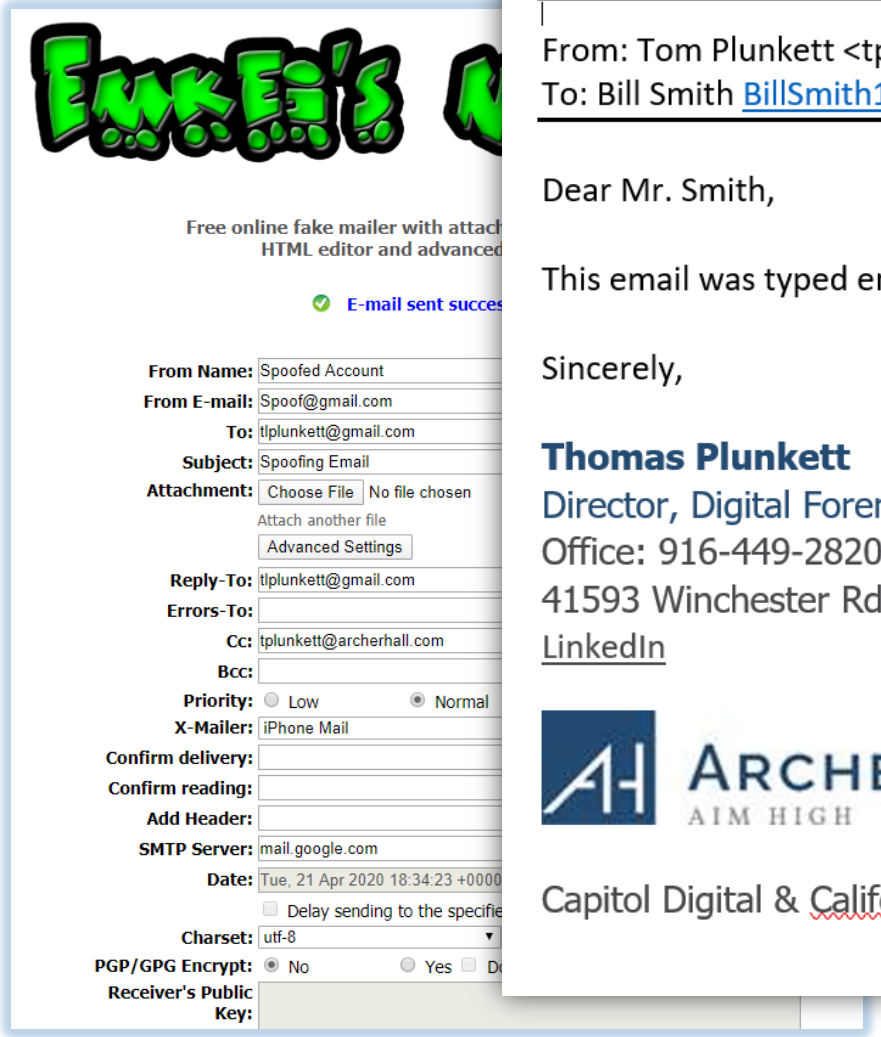
- Ruling: Admissible.
  "[T]he rules of evidence do not limit what type of information an expert may rely upon in reaching his opinion; even if that information would not otherwise be admissible in a court proceeding, an expert witness may rely upon it so long as it is the type of information on which others in the field reasonably rely. Indeed, Rule 703 now expressly permits the expert to disclose such information to the jury, provided the court is satisfied that its helpfulness in evaluating the expert's opinion substantially outweighs its prejudicial effect."
  Boim v. Holy Land Found. for Relief & Dev., 549 F.3d 685, 703 (7th Cir. 2008)

Emails

- Defendants involved in a business with the name “MTE”
- Email sent from “mte_123@Hotmail.com” with name sender name “Hayward Borders,” a board member of MTE
- At trial, no one could say they saw Borders author the emails
- Content of the emails consistent with defendant’s prior actions
- Emails contained facts known by the defendants

- Ruling: Admissible.
- “Authentication can be established in a variety of ways, including…Rule 901(b)(1), … by distinctive characteristics such as ‘appearance, contents, substance, [or] internal patterns … taken in conjunction with circumstances.” *United States v. Fluker*, 698 F.3d 988, 999 (7th Cir. 2012)

Fake Email



THIS IS A WORD DOC

From: Tom Plunkett <tplunkett@archerhall.com> Friday, April 24, 10:50 AM PDT
To: Bill Smith BillSmith15@billco.com

Dear Mr. Smith,

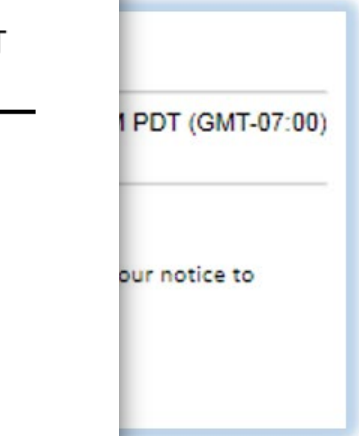
This email was typed entirely in Word and is not actually an email.

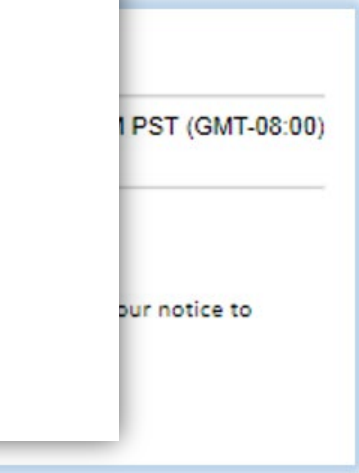
Sincerely,

Thomas Plunkett
Director, Digital Forensics
Office: 916-449-2820 | Direct: 619-276-8411
41593 Winchester Rd, Suite 151, Temecula, CA 92590
LinkedIn

ARCHERHALL
AIM HIGH

Capitol Digital & Califorensics is now ArcherHall. Learn more about our rebranding here.





Emails

Ways to truly authenticate an email:

- Retrieve original from the computer
- A witness who saw someone type the email
- Subpoena/Warrant to the email provider (Google, Microsoft, etc.)
- Trace IP address of the person logged in

Photos of Text Messages

- Pictures of text messages from an informant's cellphone
- Taken by a police officer
- Officer testified he was with the informant when she was texting
- Officer testified he saw her send and receive the text messages with "Joseph Davis"
- No evidence presented that the "Joseph Davis" contact was the same phone number as the defendant's number
- Text exchange described a location where the defendant later showed up

- Ruling: Admissible.
- [W]e require only a prima facie showing that the "true author" is who the proponent claims it to be. And the prima facie showing "may be accomplished largely by offering circumstantial evidence that the documents in question are what they purport to be."
  United States v. Davis, 918 F.3d 397, 402 (4th Cir.), cert. denied, 140 S. Ct. 202, 205 L. Ed. 2d 103 (2019)

Facebook and Text Messages

- Printout of Facebook Messages and Text Messages alleged to be from the defendant
- Defendant is quadriplegic
- Witness testified that defendant can operate a phone using his mouth and limited movement in his right arm
- Witness testified that the Facebook messages matched the defendant's manner of communicating
- Witness said she had spoken to the defendant on the phone and that phone number matched the number of the text messages
- Witness said she had seen the defendant use the Facebook account.

- Ruling: Admissible.
  "[C]onclusive proof of authenticity is not required for the admission of disputed evidence." *United States v. Barnes*, 803 F.3d 209, 217 (5th Cir. 2015)

Text Messages

- Text messages between defendant and victim, transcribed by probation officer
- Probation officer could not recall the program used to view the messages
- Forensic exam of the cell phone did not find the text messages
- Phone was registered to defendant's mother
- Probation officer said defendant admitted the messages were between him and the victim
- In a jail call, defendant mentioned the victim's phone number

- Ruling: Admissible.
- "The trial court 'does not determine whether the evidence is authentic, but only whether evidence exists from which the jury could reasonably conclude that it is authentic. [A] flexible approach is appropriate, allowing a trial court to consider the unique facts and circumstances in each case—and the purpose for which the evidence is being offered—in deciding whether the evidence has been properly authenticated.'" *State v. Fell*, 242 Ariz. 134, 136, 393 P.3d 475, 477 (Ct. App. 2017)

Facebook Messages

- Sale of stolen iPads
- Law Enforcement obtains from Facebook messages between the defendant and a third party
- Messages include picture of stolen iPad with a matching serial number
- State attempts to admit the records under 803(6) and 902(11) or (12)
- "Contrary to the State's assertion, it did not satisfy Rule 803(6)'s foundation requirements to admit the message. The State acknowledged at trial it had no certification from Facebook."

- Ruling: Admissible.
- "Authenticated statements made by and offered against a party-opponent are "not hearsay." Ariz. R. Evid. 801(d)(2)... [T]he superior court did not abuse its discretion in admitting the message so long as the record contains evidence from which a jury could reasonably conclude that the message was what the State claimed it to be—a message authored by [the defendant] himself.
  State v. Griffith, 247 Ariz. 361, 365, 449 P.3d 353, 357 (Ct. App. 2019)

State v. Griffith

- "[T]he State claimed the message was sent by Griffith himself, the State was required to provide "some indicia of authorship" to satisfy its authentication obligation before the message could be admitted into evidence."
- "A Facebook records custodian, however, could provide no such indicia beyond attesting or certifying that the message came to or from a particular account."
- "Allowing the State to fulfill "its authentication obligation simply by submitting such [a certification or] attestation would amount to holding that social media evidence need not be subjected to a 'relevance' assessment prior to admission" under Rule 803(6)."
- "Accordingly, we conclude that social media communications, when offered to prove the truth of what a user said, fall outside the scope of Rule 803(6), and thus are not self-authenticating under Rule 902(11) when offered for that purpose."

Some Tips

- **Think about admissibility when gathering the evidence**
  - Expert vs. investigator vs. witness/party vs. certification from provider
- **Decide if you should make pretrial or trial challenges to the evidence**
  - Consider demonstrating for the judge or jury how easy it is to manipulate digital evidence
- **Use pretrial interviews/depositions for authentication**
  - Ask to confirm ownership of social media accounts
  - Confirm who has access to accounts
  - Confirm personal information found on those accounts

We’d love to hear from you!

Brian M. Chase, Esq.
Managing Director
Digital Forensics and eDiscovery

bchase@archerhall.com
(855) 839-9084

ARCHERHALL
AIM HIGH