Identity and Sufficiency of Digital Evidence

Michael Losavio

Chapter 2

IDENTITY AND SUFFICIENCY OF DIGITAL EVIDENCE

Michael Losavio

Abstract Digital evidence proffered by prosecutors is subject to the same standards as all other evidence. However, a major concern is that the novelty of digital evidence may lead to less rigor in its application. This chapter discusses issues related to identity and sufficiency of digital evidence, including the need for authenticity and reliability, and concerns about identification via digital evidence.

Keywords: Digital evidence, identification, authentication, hearsay

1. Introduction

The identification of the responsible party is a core issue in all criminal investigations and prosecutions, including the pursuit of computer and online misconduct. Indeed, the identification of the person who committed the offense is an essential element that the government must establish beyond a reasonable doubt (United States v. Alexander [7]). However, this may be especially challenging for computer and online misconduct because evidence used for identification is often circumstantial or indirect rather than direct (e.g., I saw him do it).

By contrast, in many cases, digital evidence may be used in support of warrants for the search and seizure of direct evidence to establish the identity of the offender. A canonical example is digital contraband such as child pornography. Information about network usage for contraband downloads, such as an IP address, is deemed sufficient for a search warrant of the physical space associated with the IP address. Finding such contraband on a person's device supports an adjudicative finding that identifies the person as the offender with knowing possession of the contraband.

But the use of such evidence to establish identification may become attenuated with other forms of computer and network activity, especially misconduct beyond the possession of digital contraband. This may increase the risk of the incorrect identification of an innocent person as the offender.

Often, other evidence may be necessary to establish linkage to the identity of the offender. One example is the use of closed-circuit television camera recordings of device access that link a person physically to the site of activity; this additional evidence can be crucial. However, when only trace identification of a defendant is found or little direct evidence identifies the culprit, the government must prove by additional, sufficient probative facts to infer a culpable rather than accidental connection.

This chapter discusses issues related to identity and sufficiency of digital evidence, including the need for authenticity and reliability, and concerns about identification via digital evidence to prove guilt.

2. Background

This section discusses the legal foundation for identification using digital evidence. It reviews jurisprudence related to circumstantial or indirect evidence obtained via traditional – non-digital – forensics. The extrapolation is key to developing best practices for the growing body of digital evidence.

In United States v. Jordan [14], the court listed additional and substantial evidence linking the defendant to artifacts of the crime where no direct witness evidence identified him. The indirect evidence included the debit card linked to the account used in the offense, a receipt for the money order used to open the account, a cell phone containing the fraudulent message and a gift card used to pay for the telephone number on the distributed fraudulent documents.

In Mikes v. Bork [10], the court found that, with only fingerprints linking a defendant to a crime, the government must show a further connection that establishes guilt.

These cases imply that in similar scenarios involving computer or online misconduct, where direct witness identification is not possible, the identification of the culprit may be proven by inferential and circumstantial evidence [16, 17]. Network traces of activity are like fingerprints, remnants of activity that may indicate a connection without defining the depth of the connection.

The comment on fingerprint-only cases in Mikes v. Bork [10] is instructive. Often, a profile of electronic data may be assembled to create

a functional equivalent of the fingerprint, but this still requires attention to sufficient inferential and circumstantial evidence to make a conclusion of guilt beyond a reasonable doubt. When a defendant has been convicted primarily on the basis of digital evidence, there was additional circumstantial evidence beyond coincident account usage or the use of the defendant's name to connect the defendant to the crime (see, e.g., United States v. Ray [13], United States v. Gonzalez [18] and United States v. Jordan [14]).

For example, in United States v. Ray [13], an email message containing contraband was connected to the defendant by additional evidence in the email, such as pictures of his children, and testimony regarding his access and control of the relevant computer services. In United States v. Gonzalez [18], the defendant engaged in health care fraud and aggravated identity theft via online billing of health insurance companies. Extensive circumstantial text messaging evidence relating to the fraud ultimately established the connection to Gonzalez.

3. Sufficient Evidence of the Act

In United States v. Fraser [11], the U.S. Federal Court of Appeals (Sixth Circuit) discussed proper attribution regarding conduct under Federal Rule of Evidence 404(b) [24]. It did so in the context of other acts such as writings (like metadata) that contain particular facts from which attribution may be inferred.

The parties argued in this case that the other act – a book that the defendant wrote – was not some sort of previous scam, but the act of writing about the scam. Specifically, the defendant did not argue that the trial court should have determined whether he had previously committed the scam described in his book *The Birth of a Criminal*. Moreover, there was no indication that the evidence was admitted for the purpose of showing that he had actually committed the scam in the past.

The trial court made the proper preliminary determination that the defendant wrote *The Birth of a Criminal*. The court noted that the book had the picture of the defendant on the cover, listed him as the author, had a copyright date of 2002, an ISBN of 2972571302 listed on `Amazon.com` and was published by Gutter Publications. The book was further authenticated by the publisher's website, which listed the defendant as the founder of *Gutter Magazine*. The trial court thus, with detailed findings, properly determined as a preliminary matter that the defendant wrote the book.

Proof of *modus operandi* may be used to demonstrate identity, such as permitting signature evidence when identity was "the largest single issue" in the case [12], yet excluding evidence because proof of a *modus operandi* is only relevant when there is an issue regarding the defendant's identity [22]. Together these offer a profile of the types of evidence of computer and network activity that may meet the threshold of sufficient evidence to establish offender identity. A prosecution may mix and match different evidentiary facts to establish who perpetrated a crime, even when direct evidence of the identity of the offender is absent.

4. Digital Identity Case Study

This section discusses a case study involving the application of evidentiary facts in an electronic fraud prosecution.

4.1 Electronic Fraud Case

A lucrative area of criminal activity is bank and credit card fraud. Electronic banking and e-commerce systems often rely on the reduction of identification to alphanumeric strings that are easily copied or forged. The growth in two-factor authentication helps reduce such misconduct, but the continued reliance on a reduced identifier set assures that these systems will be targets of criminal activity.

One criminal case involved multiple acts of bank and credit card fraud [23]. Online applications for loans, drawdowns of loan funds and credit card and debit card use were conducted using online electronic identification. A related series of acts relating to bank fraud and unauthorized access to automated teller machines (ATMs) included the coincidence of ATM access transactions with photographs maintained by the devices with timestamps of transactions. The configurations of the ATM systems with cameras provided direct time-stamped photographic evidence that identified the culprit. However, beyond the ATM transactions with photographs, there was no other evidence to correlate or identify who was using the debit card for the other transactions and was conducting fraudulent online loan applications and withdrawal actions.

To remedy the gap, the prosecution offered evidence from a senior bank fraud analyst of an online loan application made using a name, date of birth and social security number of a putative relative as the contact and a contact email. The bank fraud analyst recommended denial of the loan application because the date of issuance of the social security number was long before the date of birth of the applicant. However, the analyst acknowledged that he could not tell from the application who was sitting at the computer when it was made.

To continue to frame the identification, another bank officer, who knew one of the victims as she worked to resolve his complaints, testified to handling an online loan application for $15,000 in the victim's name. She also testified to calling the telephone number on the application in order to speak with the fraud victim:

```
"A young gentleman answered the phone."

"He said 'hold on a second' and came back.
It was the same person I asked to talk to Mr. Victim-1 before."

"So I proceeded with the conversation.
I said, 'Victim-1?' and he said 'Yes.'"

"This is a bank officer calling.
I see that you have applied for a $15,000 premier loan with us.
It is approved so I just want to see when you want to come in
and close the loan."

Q. "What did the person on the other end say?"
A. "The person said, 'I'll be in tomorrow.'"

"I said, 'Okay. Come in with your ID.
You'll need to come into the branch and sign.'"

"At that point the person said, 'I have to come to the branch?'"

"I said, 'Yes. You have to bring your ID.
I have to enter it into the computer.'"

"He said, 'Okay. I'll be there tomorrow.'"

Q. "Did the person ever show up?"
A. "No."

Q. "Did the loan ever close?"
A. "No."
```

Additional evidence relating to these indirect actions came from another bank officer, who acknowledged an account note on the compromised joint checking account that said "Victim-1 has verified for [the defendant] to cash checks to $500. Please contact Victim-1 with any questions and ID [the defendant]."

Nevertheless, upon considering all the circumstantial factors relating to misconduct, the identification of the wrongdoer in this case was deemed sufficient by the court (United States v. Vance [21]).

4.2 Fraud Case Analysis

The criminal charging document (indictment) asserted that the defendant used the social security number of another person as the means of identification. The trial court found that the defendant used Victim-1's social security number as a means of identification to open a bank account.

Victim-1 testified that he did not give the defendant permission to use his social security number to open the account. The trial court asserted that the defendant, when using Victim-1's social security number to open the checking account and submit an online loan application in his own name with Victim-1's social security number, was attempting to commit bank fraud.

However, there was little to no evidence to support the finding that defendant had used Victim-1's social security number. The transactions were done in an anonymous manner with insufficient direct connection to the defendant. Indeed, the analysis of the trial court that supported the identification of the defendant as the offender would appear to have gaps.

Despite the fact that no direct evidence connected the defendant to the bank application, the trial court found "sufficient circumstantial evidence that [the defendant] had made the loan application."

Although the business records from the bank and the cable records, which were submitted a few days after the bench trial concluded, and although the records showed that the loan application was submitted from an IP address registered to [another person] and not the defendant, the court concluded there was sufficient circumstantial evidence that it was the defendant, as opposed to someone else, who submitted the loan application using Victim-1's social security number.

Significantly, as it relates to the charge, neither the defendant nor any other defense witness admitted to applying for a loan at the bank in the defendant's name with Victim-1's social security number. In fact, it would have been very odd for someone else to do this.

In effect, the trial court found that, although the IP address used for the fraudulent transactions belonged to someone other than the defendant and there was no direct evidence associating the defendant with the transactions, it is significant and relevant to the defendant's guilt that no one else admitted to the crime. This would appear to violate the basic tenets of a criminal prosecution where the state must prove guilt instead of a defendant having to prove innocence.

The trial court maintained that there was certainly circumstantial evidence from which the court could conclude that the defendant com-

mitted the offense of attempted bank fraud when he requested a loan in his own name using someone else's social security number. By using Victim-1's social security number, the defendant was certainly aware that, perhaps, if he had used his own social security number, he would have been unable to obtain the loan because his credit score was not high enough or he could have been denied the loan for some other reason.

Ultimately, the court found that the defendant did attempt to commit bank fraud and that he used some other person's identification during and in relation to the attempted bank fraud. The court concluded that the prosecution had submitted sufficient evidence beyond a reasonable doubt and, therefore, the defendant was found guilty.

In the pursuit of justice, the challenge is to collect and present sufficient evidence to establish guilt or, conversely, show innocence. Beyond this is the reliability of the evidence and the result – avoiding the false positive of convicting an innocent person or the false negative of acquitting a guilty party.

4.3 Sufficiency for Identification

Is there support for the trial court's factual findings about the online identity of the offender? That someone else did not confess to the offense or even that evidence did not point to anyone else do not support that the defendant committed the offense. Given the identity problems with online activities, it is just as likely that the defendant's means of identification – his name – was misappropriated by others. This fundamental failure to sufficiently establish that the defendant committed the act establishes that he should not have been convicted of the crime.

Issues of identity in an online context are significant, leading to the need for greater evidence of real identity in all online contexts using a variety of tools [2]. There was little or no evidence to support the finding that the defendant himself had used Victim-1's social security number. It was all done in an anonymous manner online with insufficient connection to the defendant. There was little or nothing that connected the defendant to the bank application. There was no authentication of the information connecting the name on the application to the real defendant according to Federal Rule of Evidence 901 [27], which requires authentication through proof that an item of evidence is what it is claimed to be.

An identification standard like this does not simply set a low bar on identification, it opens identification to error and manipulation. This case study suggests how false trails of evidence could be created to lead to innocent parties. Unfortunately, many motives are present for such

seemingly pointless malice. Harassment, often of a former spouse or significant other, would be a prime beneficiary of this standard of identification proof without connection. That a jury may decide beyond a reasonable doubt is not sufficient protection. U.S. law states that a judge must dismiss if no rational trier of fact could find proof beyond a reasonable doubt [28]. This is critical as online criminality continues to grow. Indeed, it is essential that adequate evidence be established to convict the guilty and protect the innocent.

5. Authentication and Hearsay Issues

Authentication is a foundational issue for any evidence, digital or otherwise, that establishes identity. To authenticate a fact in evidence is to demonstrate that it is what it is claimed to be. A digital artifact from social media with a defendant's name and photograph must have sufficient facts to authenticate the printout with the name and photograph. In the United States, this is covered by Federal Rule of Evidence 901(a) [8]. For example, evidence of website postings has been held to be insufficiently authenticated when the party offering the evidence failed to show that the sponsoring organization of the website actually posted the statements instead of a third party [9].

The hearsay rule relates to reliability and testability. According to Federal Rule of Evidence 801(c) [25], hearsay is "a statement that: (i) the declarant does not make while testifying at the current trial or hearing; and (ii) a party offers in evidence to prove the truth of the matter asserted in the statement." A U.S. federal court [15] has held that video purporting to demonstrate proper medical procedures was a "statement" offered for the "truth of the matter asserted" under Federal Rule of Evidence 801 [25] and, thus, its admission was impermissible hearsay (error harmless). In a related discussion about the reliability of online artifacts and their authentication as ancient documents per Federal Rule of Evidence 803(16) [26], which assumes age brings reliability, the United States Judicial Committee on Rules of Practice and Procedure noted that "[c]ommittee members unanimously agreed that Rule 803(16) was problematic, as it was based on the false premise that authenticity of a document means that the assertions in the document are reliable – this is patently not the case."

In another case [19], social media postings of pictures of a defendant with a gun, guns and marijuana were out-or-court "statements" that the defendant illegally possessed a firearm as well as drugs, guns and money. This is a multiple hearsay issue because the photographs are statements in themselves that are restated by their posting on Facebook for viewing,

restated again by their printouts and restated yet again to the jury. In this case, no foundation was made about the form of the statements or that the statements were made by the defendant. The jury ultimately found that the photographs constituted evidence of the defendant's offense because their admission materially impacted the outcome of the prosecution to prove guilt.

6. Identification in Online Environments

The challenges to identification using computer and network activity are serious and they may lead to erroneous findings. The errors cut towards the conviction of the innocent as well as the exoneration of the guilty. These are unjust and damaging to the credibility of identification, undermining its utility even as online misconduct grows. It creates an expanded tool for serious and disruptive crimes against all people through the use of forged information and "fake news." The harm from such online misinformation includes harassment, reputation damage and information fraud. Commercial services such as Reputation Defender [4] have been created to alleviate this problem.

In 2008, then vice-presidential candidate Sarah Palin was targeted by online impersonators who sent people to her home for a barbecue [29]. Online impersonation has led to the enactment of criminal prohibitions against online harassment through impersonation [6].

As digital forensics leverages artificial intelligence, machine learning and data mining, more challenges will arise that must be addressed before the innocent are hurt. The Los Angeles Police Department has suspended the use of predictive policing tools due to inconsistent implementation [5]. A law enforcement technology vendor recently empaneled experts to review the use of artificial intelligence for policing, only to have the panel advise against any implementation using available technologies [1]. An algorithm-driven, robo-adjudication, anti-fraud system was found to produce erroneous decisions in more than 80% of fraud determinations before it was suspended, albeit after causing financial damage to many people [20]. Each of these presents questions of accuracy, reliability and justice. Each of these offers significant, if not essential, support for public safety in this online era.

Failure to address the potential problems posed by advanced technologies will undermine law enforcement activities as well as public safety. Strong steps must be taken or the future may well be dystopian [3].

7. Conclusions

The identification of online criminals has been a troublesome issue over the entire lifetime of digital forensics. Increased online criminal activity, whether domestic or transnational, exacerbates the challenges to identifying the true entities responsible for crimes. The allure of simple, alphanumeric authentication and identification for online transactions has contributed to the explosion of cyber crime. Nevertheless, the need to prosecute criminals should not weaken the resolve to ensure that the right persons are held responsible for their crimes. It is imperative that protocols are created for the accurate identification and authentication of online misconduct and online miscreants.

References

[1] Axon AI and Policing Technology Ethics Board, First Report of the Axon AI and Policing Technology Ethics Board, Axon, Scottsdale, Arizona, 2019.

[2] J. Blue, J. Condell, T. Lunney and E. Furey, Bayesian-chain: Intelligent identity authentication, *Proceedings of the Twenty-Ninth Irish Signals and Systems Conference*, 2018.

[3] T. Maughan, *Infinite Detail*, Farrar, Straus and Giroux, New York, 2019.

[4] Reputation Defender, About Reputation Defender, Redwood City, California (`www.reputationdefender.com/about`), 2020.

[5] M. Smith, Review of Selected Los Angeles Police Department Data-Driven Policing Strategies, BPC #19-0072, Office of the Inspector General, Los Angeles Police Commission, Los Angeles, California (`www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf`), 2019.

[6] State of Texas, Texas Penal Code §33.07. Online impersonation, Austin, Texas (`codes.findlaw.com/tx/penal-code/penal-sect-33-07.html`), 2020.

[7] United States Court of Appeals (Ninth Circuit), United States v. Alexander, *Federal Reporter, Third Series*, vol. 48, pp. 1477–1484, 1995.

[8] United States Court of Appeals (Second Circuit), United States v. Vayner, *Federal Reporter, Third Series*, vol. 769, pp. 125–131, 2014.

[9] United States Court of Appeals (Seventh Circuit), United States v. Jackson, *Federal Reporter, Third Series*, vol. 208, pp. 633–637, 2000.

[10] United States Court of Appeals (Sixth Circuit), Mikes v. Bork, *Federal Reporter, Second Series*, vol. 947, pp. 353–361, 1991.

[11] United States Court of Appeals (Sixth Circuit), United States v. Fraser, *Federal Reporter, Third Series*, vol. 448, pp. 833–842, 2006.

[12] United States Court of Appeals (Sixth Circuit), United States v. Perry, *Federal Reporter, Third Series*, vol. 438, pp. 642–652, 2006.

[13] United States Court of Appeals (Sixth Circuit), United States v. Ray, *Federal Appendix*, vol. 189, pp. 436, 449–450, 2006.

[14] United States Court of Appeals (Sixth Circuit), United States v. Jordan, *Federal Reporter, Third Series*, vol. 544, pp. 656–671, 2008.

[15] United States Court of Appeals (Sixth Circuit), United States v. Martinez, *Federal Reporter, Third Series*, vol. 588, pp. 301–317, 2009.

[16] United States Court of Appeals (Sixth Circuit), United States v. Boyd, *Federal Appendix*, vol. 447, pp. 684–690, 2011.

[17] United States Court of Appeals (Sixth Circuit), United States v. Davis, *Federal Appendix*, vol. 531, pp. 601–607, 2013.

[18] United States Court of Appeals (Sixth Circuit), United States v. Gonzalez, *Federal Appendix*, vol. 560, pp. 554–559, 2014.

[19] United States Court of Appeals (Sixth Circuit), United States v. Farrad, *Federal Reporter, Third Series*, vol. 895, pp. 859, 875–880, 2018.

[20] United States Court of Appeals (Sixth Circuit), Cahoo et al. v. SAS Analytics Inc. et al., *Federal Reporter, Third Series*, vol. 912, pp. 887–897, 2019.

[21] United States Court of Appeals (Sixth Circuit), United States v. Vance, No. 19-5160, Decided and Filed, April 17, 2020.

[22] United States Court of Appeals (Tenth Circuit), Chavez v. City of Albuquerque, *Federal Reporter, Third Series*, vol. 402, pp. 1039–1046, 2005.

[23] United States District Court (Eastern District of Kentucky), United States v. Vance, Transcript of Trial, Case No. 18-CR-10, R. 72, Ewald, Transcript of Trial, 9/5/2018, pp 48–49, 2018.

[24] United States Government, Rule 404. Character evidence; crimes or other acts, Federal Rules of Evidence, Washington, DC (`www.law.cornell.edu/rules/fre/rule_404`), 2020.

[25] United States Government, Rule 801. Definitions that apply to this article; exclusions from hearsay, Federal Rules of Evidence, Washington, DC (`www.law.cornell.edu/rules/fre/rule_801`), 2020.

[26] United States Government, Rule 803. Exceptions to the rule against hearsay, Federal Rules of Evidence, Washington, DC (www.law.cornell.edu/rules/fre/rule_803), 2020.

[27] United States Government, Rule 901. Authenticating or identifying evidence, Federal Rules of Evidence, Washington, DC (www.law.cornell.edu/rules/fre/rule_901), 2020.

[28] United States Supreme Court, Jackson v. Virginia, *U.S. Supreme Court*, vol. 443, pp. 307–339, 1979.

[29] J. Velasco, Four Case Studies in Fraud: Social Media and Identity Theft, *Socialnomics Blog* (socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft), January 13, 2016.