AI Evidence

Don Vilfer, JD, MCFE

1

Who We Are

- Former FBI, non-practicing attorneys.
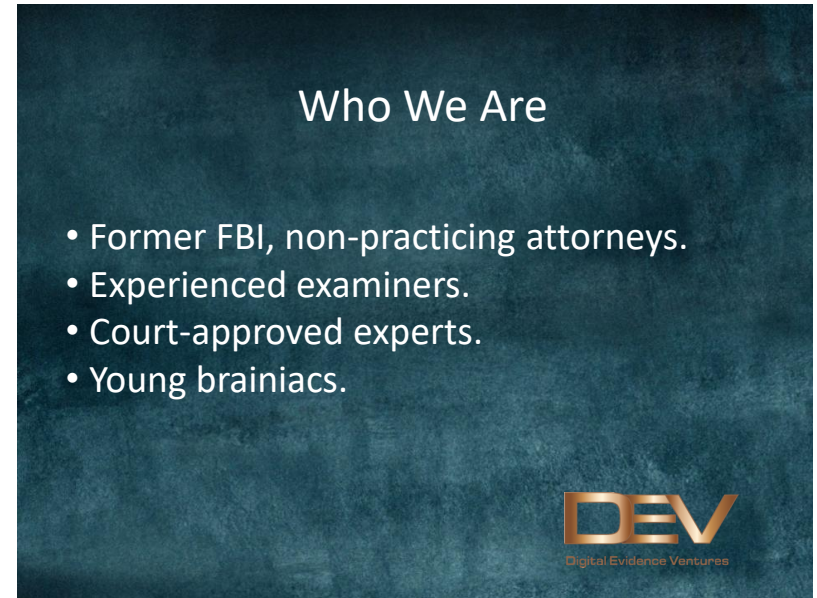- Experienced examiners.
- Court-approved experts.
- Young brainiacs.

2

Representative Clients

- Financial institutions.
- Government agencies.
- Schools and universities.
- Law firms.
- Businesses.

DEV
Digital Evidence Ventures

3

Representative Cases

- Investigation of crimes to refer for prosecution.
- Employee misconduct.
- Title IX investigations for universities.
- Criminal defense.
- Sexual harassment.
- Incident response-hacking.
- Theft of trade secrets.

DEV
Digital Evidence Ventures

4

2

What We Will Cover

- What is AI.
- How can it be used to mislead.
- Case examples.
- Detection and blocking the use of fake evidence with existing law.

DEV
Digital Evidence Ventures

5

What is AI?

- A term used since the 1950s.
- Using computers to simulate human intelligence.
- Machine Learning: Ingest large amounts of data and analyze for patterns.
- Generative AI: Generate new data based on the learning.

DEV
Digital Evidence Ventures

6

Popular AI Sites

- ChatGPT - AI-powered language model capable of generating human-like text based on context and past conversations.
- DALL-E 2- Created by makers of ChatGPT. Users enter text to generate images.
- Canva.com- Free AI photo generator.
- Voice Generators- Speechify (offers voice cloning), Play.ht.

7

AI Generated Photo Example

- Prompt: an accurate photo of a tesla on fire in San Francisco.

8

4
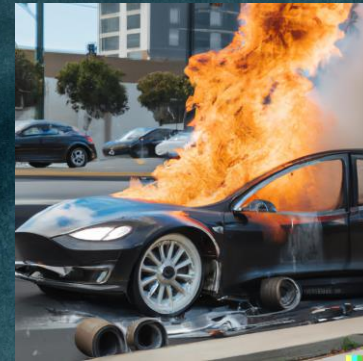
Why Would Anyone Mislead You?

- Revenge.
- Gain an advantage in litigation or pre-litigation.
- Cover their own misdeeds or mistakes.
- Eliminate a business partner.
- Get rid of a significant other.

DEV
Digital Evidence Ventures

9

Beware Non-Digital, Digital Evidence

- The printed email.
- The printed text message (or selected messages).
- The screenshot of a text conversation.
- The alibi photo on paper.
- The "copy" of the original (photo, tape, files).

DEV
Digital Evidence Ventures

10

5

Case Law re Non-Digital Evidence

State v. Kolanowski, (Wash: Court of Appeals, January 30, 2017). In a case involving the failure to authenticate social media evidence, a criminal defendant unsuccessfully sought to admit a screenshot of Facebook evidence that he maintained would have served as critical impeachment of the prosecutions' main witness. The State successfully argued the screenshot lacked foundation. Metadata that could have been obtained during the collection was not obtained—a simple screenshot did not suffice.

11

Thwarting AI Evidence via Traditional Forensics and Rules of Evidence

- Tried and true forensic and legal methods

12

What is Digital Forensics?

- Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. --Wikipedia

13

The Usual Rules of Evidence Still Apply

- Chain of Custody – must be able to account for the location of the evidence from the moment it was collected. Can it be proven to come from the source represented?

- Authentication – computer evidence is considered "writings and recordings" under the Rules of Evidence and must be authenticated to be admissible.

- Validation – is it really the same? (Hash files)

14

Forensic Image

- The creation of a Forensic Duplicate of the storage media. (Cell Phone "extractions")

- FRE Section 1003: a duplicate is admissible to the same extent as the original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

- California Evidence Code Section 1521.

- In using forensic copies to challenge suspect evidence, we can get our info admitted.

15

Characteristics of a Forensic Image

- Hash value (digital fingerprint).
- Data cannot be changed.
- Includes unallocated space, drive freespace and file slack.
- Difference from Ghost.
- Acceptable in court as best evidence.

16

A Primer on Cell Phone Forensics Techniques to Validate Evidence

- Validation that artifacts are real (handle ID)
- Communication between subjects/witnesses
- Provide location during key times
- Tying artifacts to carrier records
- WiFi connections or offered connections
- Use of time

DEV
Digital Evidence Ventures

17

Do Not Let My Ex Out of Jail Again!

- Ex boyfriend calls police and shows threatening text on his cell phone.
- Police take photo of message and arrest ex-girlfriend.
- Girl makes bail, boy calls police again and shows printed email threat, police arrest girl again.
- Expert review shows alleged text in photo is not formatted like that phone model. Boy had someone send message starting with her phone number. Phone records show no sent text from her. No sent email from her email. Boy confesses and is arrested.
- What could have been done differently?

DEV
Digital Evidence Ventures

18

The Case of Many Signs

- Motorcyclist injured in poorly marked construction zone.
- Plaintiff claims he saw no signs.
- Defendant submits photos of area with lots of warning signs.
- Forensic analysis of photos establishes faked-traditional forensic methods used.

DEV
Digital Evidence Ventures

19

The Case of the Racist Detective

- Criminal defendant charged with luring minor via text messages.
- Defendant produces digital evidence to his attorney - text messages and a voice message from assigned detective.
- Defense attorney is suspicious and retains us to evaluate evidence.
- Messages and voicemail were faked-how we determined and what attorney did.

DEV
Digital Evidence Ventures

20

Challenges to Fake Evidence May Not Be Immediately Accepted Without Evidence

Tesla attorneys sought to block use of a video of Musk making safety claims of self-driving car.

Judge ordered Musk to testify to the issue under oath and wrote "What Tesla is contending is deeply troubling to the Court... Their position is that because Mr. Musk is famous and might be more of a target for deep fakes, his public statements are immune. In other words, Mr. Musk, and others in his position, can simply say whatever they like in the public domain, then hide behind the potential for their recorded statements being a deep fake to avoid taking ownership of what they did actually say and do. The Court is unwilling to set such a precedent by condoning Tesla's approach here."

DEV
Digital Evidence Ventures

21

Side Note-Do Not Rely on AI for your Legal Briefings

Judge P. Kevin Castel wrote regarding a plaintiff's filing that "six of the submitted cases appear to be bogus judicial decisions with bogus quotes and bogus internal citations." He called it "an unprecedented circumstance."

In his affidavit filed later, counsel said ChatGPT not only provided the legal sources, but assured him of the reliability of the opinions and citation that the court has called into question.

DEV
Digital Evidence Ventures

22

23