

THE CASE FILE · NO. 1

How Evidence Gets Manufactured

*The real forensics behind The Edited Truth Series. None of it is
invented.*

TIFFANY TORRES

THE EDITED TRUTH SERIES

Before you start

Every novel I write begins with the same question. If you were shown a piece of evidence that looked completely real, how would you know?

Not "would you believe it." You would. That's the point. The question is whether you'd have any way to check.

What follows is the real science underneath the fiction. None of it is invented. Every technique in this guide is documented in forensic literature, court records, or published research. I've stripped out the jargon and kept the parts that matter.

Some of this will make you uncomfortable. Good. It should.



1. Video: the thing your eyes are worst at

We treat video as the gold standard. Seeing is believing. It's the most trusted evidence in an American courtroom and the easiest to doubt once you understand how it's made.

Digital video isn't a recording of reality. It's a reconstruction. Your camera throws away most of what it sees, keeps a fraction, and rebuilds the rest using math. That reconstruction process leaves fingerprints, and those fingerprints are where the truth lives.

What analysts actually look for:

Compression artifacts. Video is compressed in blocks. When someone alters a region of a frame and re-saves it, that region gets compressed twice while everything around it was compressed once. The doubled area carries a subtly different noise signature. It's invisible to your eye and obvious to software.

Sensor noise. Every camera sensor has a unique pattern of imperfection, a sort of birthmark, technically called photo-response non-uniformity. It's consistent across everything that camera records. If a section of frame lacks the pattern, or carries a different one, that section didn't come from this camera.

Physics that doesn't hold. Shadows falling at angles that don't agree with each other. Reflections that don't match the room. A light source that brightens one object and not the one beside it. Compositing is very good now. Lighting physics is still hard.

Temporal inconsistency. Real motion is continuous. A person's hand moves through every position between here and there. Synthesized motion tends to be smoother than reality, or to skip in ways a body doesn't.

The thing worth knowing: the hardest video to question is live video. We assume a livestream is real because it's happening now, and "now" feels unfalsifiable. It isn't. A stream is a signal traveling from a camera to a server to your screen, and anywhere along that path is somewhere a signal can be changed.

1. VIDEO: THE THING YOUR EYES ARE WORST AT



2. Audio: the voice is not the person

Voice synthesis got good fast. A few years ago you needed hours of a person's speech to clone their voice. Now a short sample can be enough for something that fools a family member on a phone call.

Which means a recording of someone's voice saying something is no longer meaningful proof they said it.

How synthetic audio gives itself away:

Room tone. Every real recording contains the sound of the space it was made in. Air handling, distant traffic, the hum of a refrigerator, the particular way that room's walls absorb sound. It's a continuous bed underneath the speech. Generated audio often has no room, or a room that doesn't change when the speaker moves.

Breathing. People breathe. They breathe in patterns shaped by their bodies, their emotions, and their health. Someone frightened breathes badly. Someone with damaged lungs breathes audibly, and can't sustain a long phrase without breaking it. Synthetic speech tends to breathe where the model learned breaths go, which is to say, in the average place, at the average rate.

Phoneme timing. Human mouths take real time to move between sounds. Certain transitions are physically slow. Generated speech can produce transitions that no anatomy could make, and it can be perfectly consistent in ways that a tired, stressed, distracted human never is.

Spectral fingerprints. Vocoder and neural synthesizers leave traces in frequency ranges above what you consciously hear. To you it's a voice. On a spectrogram it can be a signature.

The thing worth knowing: the weakness of a fake isn't the voice. It's everything around the voice. Faking a person is easy now. Faking a room, a body, and a moment all at once is still hard.



3. Chain of custody: the boring thing that decides cases

Here's the part nobody puts in a trailer. Most evidence isn't defeated by proving it's fake. It's defeated by proving nobody can account for where it's been.

Chain of custody is the documented history of a piece of evidence from the moment it's collected to the moment it's shown to a jury. Who touched it. When. Where it was stored. Who moved it and why. Every transfer signed.

It exists because evidence is physical, and physical things can be swapped, contaminated, mislabeled, or lost. The chain is the only thing standing between "this is the knife from the scene" and "this is a knife."

Where chains break in real life:

Time gaps. An item is logged out at 2:40 and logged in at 6:15 and nothing explains the intervening hours.

Bulk logging. Forty items entered at the identical timestamp, which means someone did the paperwork later from memory.

Unnamed hands. A transfer recorded to a department rather than a person.

Storage that isn't secure. A refrigerator, a shelf, a room that a dozen people have keys to.

The modern problem: chains are digital now. That's mostly an improvement. Digital logs are timestamped automatically and harder to lose. But a paper log has to be altered by a human being with a pen, and every alteration leaves a mark. A database record can be changed by anyone with the right permissions, and if the system doesn't keep an immutable audit trail, the changed record looks exactly like a record that was always that way.

The paper trail was harder to fake than the digital one. That's not nostalgia. That's a design flaw we walked into on purpose.



4. DNA: the most trusted number in the room

Juries hear "DNA match" and stop listening. Understandable. It sounds like arithmetic, and arithmetic doesn't lie.

DNA is genuinely powerful evidence. It's also more interpretive than almost anyone outside a lab realizes.

Single-source DNA is the strong case. One person's genetic material, good quantity, clean sample. Match statistics here can be staggering and deserved.

Mixtures are where it gets difficult. Most real-world samples contain DNA from more than one person. Now an analyst has to decide how many contributors there are, which markers belong to which person, and which faint signals are real versus noise. Different analysts looking at the same mixture have reached different conclusions. That's not misconduct. That's the nature of the work.

Trace and touch DNA compounds the problem. We shed genetic material constantly. Your DNA can reach a place you've never been, carried on an object, a hand, a fabric. There are documented cases of people linked by DNA to scenes they had no connection to.

Terms worth knowing:

Cold hit. A sample searched against a database returns a name, with no other investigative reason to suspect that person. Databases are large. Searching a large database changes the statistical meaning of a match, and that adjustment is not always explained to a jury.

Probabilistic genotyping. Software that interprets complex mixtures by modeling probability. Widely used, genuinely useful, and often proprietary, which means defense experts have sometimes been refused access to the source code that produced the number a jury will hear.

Contamination. DNA moves. It moves in labs too, on gloves, on surfaces, through the air in aerosolized form. Labs have documented cases of contamination from staff, from other cases, and from reference samples.

The thing worth knowing: DNA doesn't tell you a person committed a crime. It tells you their genetic material was somewhere. Everything between those two statements is interpretation, and interpretation is where cases are made.



5. Eyewitnesses: memory is not a recording

Eyewitness misidentification is a factor in the majority of DNA-based exonerations in the United States. That's not a small effect. It's the single largest documented contributor to proven wrongful convictions.

The reason isn't that witnesses lie. Most don't. It's that memory doesn't work the way we assume.

Memory is reconstructive. Every time you recall something, you rebuild it, and the rebuild is influenced by everything you've learned since. That includes what an officer said, what another witness mentioned, what you saw on the news, and what you've told yourself in the eleven months since it happened.

How honest memory gets corrupted:

Confirming feedback. A witness picks someone out and is told, in words or in tone, that they picked the right person. Their confidence rises sharply, and confidence is what juries actually respond to. Their memory of how certain they'd been at the time rises too.

Repeated interviewing. Each retelling smooths the account. Uncertainty falls away. Details firm up. The story gets better, and "better" means more confident, not more accurate.

Suggestive procedure. A lineup where one person stands out. An officer who knows the suspect and administers the lineup anyway. This is why blind administration exists, and why it isn't universal.

Cross-witness contamination. Two witnesses talk. Now they have one memory between them, and neither knows which parts were originally theirs.

The line worth understanding: there's legitimate witness preparation and there's coaching, and they're on a spectrum, not opposite sides of a wall. Telling a nervous witness where to sit and what the process will feel like is proper and necessary. Walking them through their account until the wording is clean and repeatable is something else. The tell is uniformity. Real memory is messy,

hedged, and specific in odd places. When two independent witnesses use the same phrases in the same order, they aren't independent anymore.



6. Metadata: the evidence about the evidence

Every digital file carries data about itself. When it was created, on what device, with what software, and often where. Photographs carry camera settings and sometimes GPS coordinates. Documents carry revision histories and author names.

Metadata is enormously useful and routinely misunderstood in both directions.

It can catch a fabrication instantly. A document supposedly written in March that has a creation date in July. A photograph whose embedded camera model doesn't match the phone it allegedly came from.

It's also trivially editable. Metadata is just fields in a file. Anyone with basic tools can change them. So metadata that incriminates is meaningful mainly when it's inconvenient for whoever produced the file, and metadata that exonerates is worth checking twice.

The useful principle: metadata is strong evidence when it's internally inconsistent, and weak evidence when it's tidy. A real file made by real people through a real process accumulates mess. Perfect provenance is a little suspicious.



7. Algorithms in the justice system: the math nobody audits

Software now shapes decisions at nearly every stage of an American criminal case. Whether someone is detained before trial. What sentence gets recommended. Where police concentrate patrols. Which cases get flagged for review.

These tools are usually described as objective. Some of them are useful. The problems are structural.

Training data carries history. A model learns from past decisions. If past policing concentrated on certain neighborhoods, the model learns those neighborhoods produce crime and recommends more attention there, which produces more recorded crime, which confirms the model. The loop is self-reinforcing and looks like evidence.

Proprietary means unexaminable. Many tools are commercial products, and vendors resist disclosing how they work, citing trade secrets. Defendants have been sentenced with reference to scores they could not meaningfully challenge because nobody outside the company could explain how the number was produced.

Validation is inconsistent. A risk instrument should be tested against real outcomes in the population where it's used. That doesn't always happen, and a tool validated on one population can behave very differently on another.

Scores get treated as facts. This is the practical danger. A number arrives with the authority of mathematics. Human judgment quietly reorganizes itself around it, and everyone involved can honestly say they were only using it as one factor.



8. Expert testimony: the credential is not the science

Juries have a hard job with experts. Two credentialed people say opposite things, and the jury has no way to evaluate the underlying discipline.

Several forensic techniques presented for decades with great confidence have since been substantially undercut by scientific review. Bite mark comparison. Certain hair microscopy conclusions. Some fire pattern interpretations. Various types of toolmark identification. People went to prison on all of them.

Questions that separate strong from weak forensic testimony:

Is there a documented error rate for this technique, and does the expert know it?

Was the analysis done blind, or did the analyst know what answer the case wanted?

Is the conclusion stated as a probability, or as a certainty? Certainty is a warning sign in most disciplines.

Has the method been validated by people who didn't invent it?

Can the underlying data and method be examined by the other side?

The thing worth knowing: the most dangerous expert isn't the dishonest one. It's the sincere one working in a field that never established how often it's wrong.



9. Why this holds together

Read those sections back and you'll notice they share a structure.

In every case, the vulnerability isn't the evidence. It's the gap between what the evidence actually proves and what everyone in the room assumes it proves.

DNA proves genetic material was present. We hear guilt.

Video proves a sensor recorded a pattern of light. We hear truth.

A recording proves a waveform exists. We hear a person speaking.

An algorithm proves a calculation ran. We hear objectivity.

That gap is where cases get made and where they get broken. It's also, if you want the honest answer, where I get my plots. I don't invent ways to fake evidence. I read the literature on how evidence fails and ask what it would look like if someone did it deliberately.



10. How to read a real case in the news

A practical habit, and the most useful thing in this guide.

Next time you follow a criminal case, try separating what's actually established from what's being asserted. Four questions do most of the work.

What does this evidence literally prove? Not what it suggests. What it establishes as fact.

Who produced it, and did they know what result was wanted? Analysis done with knowledge of the desired answer is analysis with a thumb on it, even when everyone is honest.

Can the other side examine the method? Not just the conclusion. The method.

What would it look like if this were wrong? If you can't imagine a version of the world where the evidence exists and the conclusion is false, you probably haven't understood the evidence yet.

That's it. That's the whole discipline, compressed.

It's also what every attorney in my books is doing, in the middle of the night, with a case file and not enough time. They aren't looking for a smoking gun. They're looking for the gap between what the record says and what actually happened.

Sometimes the gap is a mistake.

Sometimes somebody put it there.



The Case File keeps growing.

New research notes, bonus scenes, and stories get added as the series does. Subscribers get every one of them, and hear about each new book first.

edenrootpress.com/tiffany-torres

Written for readers. This is general information, not legal advice, and not a substitute for a licensed attorney. Forensic standards and criminal procedure vary by jurisdiction. If you have a real legal matter, talk to a real lawyer.

MORE FROM TIFFANY TORRES

The Case File

Three more case files over two weeks, then the novels. Ten pieces of evidence with ten hidden problems, a defence field guide, and the one word in an official record that changed everything.

Case File No. 2 - Can You Spot the Edit?

Ten pieces of evidence. Ten hidden problems. Answers at the back.

Case File No. 3 - The Defense Field Guide

The courtroom is not where most cases are decided.

Case File No. 4 - The Record

One word in the official record was wrong, and it held.

The Novels Go Further

Where the case files stop and the fiction starts.

Choose Your Case

Which part of the system would you trust least?

OPEN THE CASE FILE

<https://edenrootpress.com/tiffany-torres-reader-vault/>