Episode Book

EPISODE #6095

How to Prove Your Photo Is Real

PUBLISHED	18 October 2026 at 12:38 UTC
DURATION	27:44
LISTEN	myweirdprompts.com/episode/prove-photo-video-authentic-14590/
HOSTS	Corn, Herman, Larry, Hilbert
SCRIPT MODEL	anthropic/claude-opus-5.5
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.10
BOOK GENERATED	19 October 2026 at 17:43 UTC

SYNOPSIS

Five years ago the risk was someone faking evidence against you. Now the bigger risk is the other side calling your real photo fake — the "liar's dividend." This episode works through how an ordinary person documents a landlord dispute, an insurance claim, or a neighborhood fight in a way that can later be shown to be authentic. It covers the four different claims people bundle together when they say "this photo is real," why Timemark's server-side Photo Codes and ProofMode's on-device cryptographic signatures solve different halves of the problem, and what happened when Nikon signed an AI image by accident and had to revoke every certificate it had ever issued. Plus: what the Pixel 10, Galaxy S25, and iPhone 18 Pro actually sign, and why video walkthroughs beat stills.

TRANSCRIPT



Corn

A little over a year ago a judge in Alameda County, California, threw out an entire lawsuit. With prejudice. The plaintiffs had backed their motion with video of a witness, and the judge found the person in it bears, her phrase, a passing resemblance to the real one. It was generated. The case is gone, and it isn't coming back.



Herman

Mendones versus Cushman and Wakefield. And the part people skip is that the same judge was looking at genuine exhibits in that case too. She had to sort the real footage from the fake footage herself, frame by frame, because nobody had given her a way to tell them apart.



Corn

Which is the problem Daniel wants solved, from the other end. He isn't asking how to catch a fake. He wants to know how an ordinary person, in a landlord dispute, an insurance claim, a fight with a neighbour, gathers photos and video that can later be shown to be real. Not generated, not tampered with. Both modalities, stills and video, because they behave very differently. He uses ProofMode and Timemark on Android and likes them, and he wants everything else. We've done the chain of custody side of this before, the write once storage and so on. This is the field guide.



Herman

The urgency is that the threat model flipped. Five years ago the risk was the other side faking something. Now the bigger risk for most people is the other side saying your real photo is fake. There's a name for it, the liar's dividend. Once everyone knows fakes are easy, anything inconvenient can be waved away.



Corn

Tesla tried it.



Herman

Huang versus Tesla, twenty twenty-three. Tesla's lawyers suggested recordings of Elon Musk talking up Autopilot might be deepfakes. The judge refused, and said if that worked, famous people would be immune from their own public statements.



Corn

A good outcome. For a man whose statements are very public. Your flat's skirting board is not.



Herman

No, and that's the gap. Corn, before I go into tools... when you picture proving a photo is real, what do you think you're actually proving? Because I think people bundle four different claims together.



Corn

I'd have said one thing. That it's what the camera saw.



Herman

That's the one nobody can fully prove, as it happens. Pull it apart. One, integrity: this file hasn't changed a single bit since it was made. Two, time: it existed at a particular moment. Three, origin: it came off a particular device's camera, not out of a generator or an editing app. And four, the scene: what's in the frame was really there. Tools are good at one and two, getting decent at three, and nothing does four.



Corn

So my photo of a damp patch can be perfectly authenticated as a photo of a printed picture of a damp patch.



Herman

Yes. The camera will sign that honestly. Which is why the human who took it still matters, we'll get there. But this four-way split is why Daniel's two apps are so different from each other.



Corn

Timemark first. I've seen these. Builders use them, delivery drivers. The time and the address stamped in big letters across the bottom of the photo.



Herman

The stamp itself is worth nothing. It's pixels. Anyone with an image editor can draw a timestamp, or crop yours off and paint on a better one. If the overlay is all you have, you have a photo with a caption.



Corn

A caption with confidence.



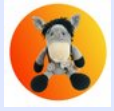
Herman

The interesting part of Timemark is the small code down the side of each photo. Fourteen characters. They call it the Photo Code. When the picture is taken, the app registers that code on Timemark's servers along with the time and the location it recorded. Anyone, your landlord, a deposit scheme, a judge's clerk, can go to their verification page, type the code or upload the photo, and get back authentic, fake, unable to verify, or not found.



Corn

So the proof isn't on the photo. It's in a database in someone else's building.



Herman

Correct, and that cuts both ways. It's independent of you, which is the strength. Timemark also refuses to issue a code if it sees the phone's clock has been changed, or a mock location app running, or on Android a modified version of the app. That's real



Herman (continued)

anti-cheating. But read their own help pages and they say plainly the check does not analyse the pixels. It confirms they issued that code and shows what time and place they stored. The marketing pages are a bit more generous about image integrity than the help pages are, and I'd believe the help pages.



Corn

If the company folds, the codes point at nothing.



Herman

The codes don't expire, but yes, the whole thing lives or dies with their servers staying up and the record staying there. For a deposit dispute that resolves in three months, fine. For a claim that runs four years, I'd want something that doesn't need anybody's permission to verify.



Corn

Which is ProofMode.



Herman

Which is ProofMode, and it's the opposite philosophy. Guardian Project, with the human rights group WITNESS, it's been in development since about twenty thirteen. The key design choice: it never touches your original file. It writes the proof beside it. A cryptographic hash of the file, SHA two fifty-six, a digital signature over that with a key that lives on your phone, and a snapshot of what the sensors knew at that moment. Location, network, device details.



Corn

Say what the hash buys me, in landlord terms.



Herman

It's a fingerprint of every bit in the file. Change one pixel, re-save it, crop it, and the fingerprint comes out completely different. So if you can show the hash existed on the day, and the file you hand over today still produces that hash, then the file hasn't been touched since. That's integrity. The signature ties the hash to your device's key. And the current versions go further, the three point x releases are C two PA conformant, so the proof can also travel inside the file in the industry format, the Content Credentials thing.



Corn

Let me guess where you're about to go. You've found the signature scheme and you're about to explain elliptic curves to me for six minutes.



Herman

I was not.



Herman

I was going to do two minutes on OpenPGP and then stop.



Corn

Do the limitation instead.



Herman

Fine. The limitation is they tell you themselves. Guardian Project says ProofMode has not had a full security or legal audit and has not been tested in court. That's admirably candid, and it matters, because a self-signed proof is you vouching for you. The key is on your phone. A sceptical lawyer will say, the person with the motive to fake this also holds the signing key.



Corn

So what does it actually get me against that lawyer?



Herman

It makes a later fake expensive. If you share the proof bundle the same day, through their share proof button, to someone else, then the hash is sitting in their inbox with their mail server's date on it. Now your story isn't "trust my phone". It's "this exact file existed on the third of May, and the landlord has had it since the third of May". That's the move, and it isn't really about ProofMode. Any file you send to the other party at the time becomes their copy too.



Corn

The landlord as my notary. He'll love that.



Herman

He doesn't have to love it, he has to have received it.

L

Larry

Are you troubled by doubt? Does your evidence keep you up at night, wondering whether it was ever really there? Ask your landlord about Verifexa. Verifexa is the once daily tablet that certifies your memories at the source, so everything you remember is cryptographically yours. Side effects may include dry mouth, mild drowsiness, and a metallic taste described by some patients as timestamped. Do not take Verifexa if you have ever been photographed. Some patients report remembering events with a valid signature that did not occur, a feeling of being watermarked from the inside, and waking at three in the morning able to recite their own hash. In rare cases, Verifexa may cause your past to be revoked by the issuing authority. If you experience a chain of custody lasting more than four hours, contact a notary. Verifexa. Because you were there. Probably.



Herman

I've got a box of those. I can tell you the hash of my own breakfast and nothing at all about Thursday.



Corn

Phones themselves, then. Daniel's on Android. Does he even need an app any more?



Herman

Depends very much which Android. The Pixel Ten, from last year, signs every photo the stock camera takes with Content Credentials. The keys sit in the security chip, the Titan M two. Google says it's the first camera app to reach what C two PA calls assurance level two, which roughly means the signing happens in hardware the operating system can't get at. It timestamps on the device so the credential survives the certificate expiring, it works offline, and they built it so your photos can't be linked to each other or to you.



Corn

And video?



Herman

I haven't seen video signing confirmed on the Pixel. Stills, yes.



Corn

Samsung?



Herman

Backwards from what you'd want. The Galaxy S twenty-five adds a credential only when you've used one of its generative AI tools on the photo. So the signed images are the edited ones, and the untouched original goes out naked.



Corn

The only photos it vouches for are the ones it helped fake.



Herman

To be fair, it's labelling, not vouching. It's telling you AI was involved. But for Daniel's purposes, a Samsung original carries nothing. Then Apple, just last month, with the iPhone eighteen Pro. From the coverage so far, there's an opt in mode where the sensor signs the pixel data itself and the phone's secure chip signs the metadata. The time doesn't come from the phone's clock at all, it comes from two timestamps Apple signs, one before and one after the shot. Stills only, main camera only, and it is not C two PA. Apple's own system, no public spec, and the usual C two PA checkers can't read it.



Corn

Of course it isn't.



Herman

Apple's own write-up, as reported, makes a line I like though. It proves what light hit the sensor. Not what the scene was.



Corn

The damp patch problem, admitted by a trillion dollar company.



Herman

It's honest, though. Here's the cautionary tale for anyone who thinks hardware signing settles everything. Nikon added C two PA signing to one of its Z cameras in August of last year. Within days a researcher found that the multiple exposure mode would sign an image the camera had never captured. He got it to sign an AI image. Nikon confirmed it, suspended the service and revoked every certificate it had issued.



Corn

Every one. So every honest photographer's signed photos...



Herman

Revoked along with the fake. And worse, a lot of the standard checking tools didn't check revocation, so the bad image still showed as valid. The signing service was still down as of February.



Corn

A camera with an alibi that turned out to be the getaway driver.



Herman

Hardware signing, then, is the strongest origin claim available, and it can still break, and when it breaks it breaks for everyone at once. Which is an argument for layering. Corn, if you were moving into a flat tomorrow, what would you actually do?



Corn

Honestly? Walk round once with the phone, take forty photos, never look at them again.



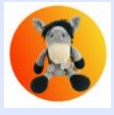
Herman

That's what everybody does. And it's the stills mindset. Video is where I'd spend most of Daniel's effort, because video has a property photos don't.



Corn

It's harder to fake?



Herman

It's harder to fake convincingly in one continuous take, yes, though that's eroding. The bigger thing is continuity. A photo of a scratch on a wall proves there's a scratch on a wall. It doesn't prove which wall. A single unbroken walkthrough, front door, hallway, each room in turn, the camera never cutting, ties every defect to its place in the flat. You can't swap in a scratch from another property without a cut, and a cut is visible.



Corn

And I narrate it.



Herman

Narrate it. Say the date, say the address, say what you're looking at. "Kitchen, left of the sink, the counter edge is chipped, that was here when I arrived." Speech gives it a second layer of content that has to line up with the picture. Some people show a phone screen with the time, or the day's news on it, at the start. That's not proof, anyone can stage it, but it costs a faker effort and it costs you nothing.



Corn

Do the whole place. Even the rooms that are fine.



Herman

Especially the rooms that are fine. Insurers say the same about car accidents. Photograph the sides of the car that aren't damaged, because otherwise there's a later argument about whether they were. Wide shot first so you can see where you are, then close. Same for a flat. And then, the part everyone gets wrong... do stills too. Not instead. Video gives continuity, stills give resolution. A frame grabbed from video of a hairline crack looks like soup.



Corn

Video soup. That's most of my move-in footage.



Herman

Now here's where video gets hard, and where Daniel should be careful. Every integrity method we've talked about depends on the file staying exactly as it was. Video is the format that gets mangled the most. Send it through WhatsApp normally and it's re-encoded, compressed, and most of the metadata is stripped. The hash breaks, the C two PA credential is gone, and the file gives no sign it ever had one. Same on Facebook, Instagram, X.



Corn

So the most common way anyone in the world shares a video destroys its proof.



Herman

Silently. Which is the nasty part. You get a perfectly playable video and nothing tells you it's been laundered of all its evidence. The workaround in WhatsApp is to send it as a document rather than as a video. Reports are that it then passes through untouched, metadata and all, up to two gigabytes. WhatsApp doesn't document that anywhere I've seen, so test it. Hash before, hash after, compare.



Corn

Is a hash a thing a normal person can do?



Herman

It's one command on a laptop, and there are free apps for phones that'll show it. Write the hash in the email when you send the file. Then the email itself records what the fingerprint was on that day.



Corn

How do the proper video tools handle it? One hash over a two gig file?



Herman

The simple apps, ProofMode, eyeWitness, yes, one hash over the finished file. C two PA for video is cleverer. It hashes the video in chunks and builds a tree of hashes, so you can check each piece without the whole stream. That's what makes signed live streaming possible. And on the pro side, Sony's Camera Verify started with stills last year and added video in March, on its bigger Alpha bodies and the FX cameras. It checks the signature, the capture time, and depth information, whether there was a real three dimensional scene in front of the lens or a flat screen.



Corn

That answers the photo of a printed photo.



Herman

For Sony's cameras, partly. For Daniel's phone, no.



Corn

Mention eyeWitness properly. You slid it in.



Herman

eyeWitness to Atrocities. Founded by the International Bar Association. Built for war crimes documentation, so it's paranoid in exactly the right ways. It records location, time, the nearby cell towers and wifi networks, hashes the footage on capture, hashes it again when it's uploaded, and compares. The upload goes to secure storage, every access is logged, and their team can supply a chain of custody statement if it goes to court. Tens of thousands of items from Ukraine alone.



Corn

For my deposit.



Herman

It's free, and it's overkill. But the design tells you what a court-grade system looks like: a second party holds the copy from the moment of capture, and you can't edit it. That's the principle even if you just use your phone and your email.



Corn

Here's the bit I actually don't know. What does a court do with any of this? Because my guess is a judge has never heard of ProofMode.



Herman

Your guess is mostly right, and it reframes the whole thing. In almost every system, a photo gets in because a person stands up and says, I took this, on this day, it fairly shows what was there. That's authentication. The witness is the authentication. The tools are corroboration for when someone attacks that.



Corn

So the app is my backup, not my case.



Herman

The app is what you reach for when the other side says it's fake. In the US there's a neat mechanism, Rule nine oh two of the federal rules, subsection fourteen, since twenty seventeen. Data copied from a device can be self-authenticating if a qualified person certifies it was verified by hash. It was written for forensic examiners, not tenants, but it tells you the legal system already treats hash matching as the way to show a copy is faithful.



Corn

And the deepfake rules people keep writing about?



Herman

Still in committee. There's a proposed new rule on machine-generated evidence, and a draft amendment for deepfakes. The draft's logic is good. The person crying deepfake has to bring something first, enough for a reasonable person to suspect fabrication. Just saying "AI" isn't enough. Then the burden swings back and the side offering the evidence has to prove it more strongly. As of their May meeting, they still hadn't adopted it.



Corn

I'm told judges are keen.



Herman

That's the funny bit. A federal judicial survey this spring found judges who'd never dealt with a deepfake were the most in favour of new rules, a bit over half. The ones who had dealt with one were much less keen, about a third.



Corn

Experience is a great cure for enthusiasm. I've watched it work on you for years.



Herman

It hasn't worked yet.



Corn

I've noticed.



Herman

Britain's version of the argument is slightly different. Courts there presume a computer was working properly unless someone shows otherwise, and the Post Office Horizon scandal, hundreds of people wrongly prosecuted on bad software, made that presumption very uncomfortable. The government consulted last year on changing it, but the proposal was aimed at evidence a program generates, not what a device simply records. An ordinary phone photo would probably sit outside it either way.



Corn

Detection. Daniel didn't ask, but everybody will. Can't I just run the other side's photo through one of those AI detector sites?



Herman

You can, and you should treat the answer like a horoscope. There's a benchmark built from deepfakes that were actually circulating in twenty twenty-four rather than the tidy academic sets. The open source detectors lost roughly half their performance on it, across video, audio and images. The commercial ones did better and still weren't as good as



Herman (continued)

trained human analysts.



Corn

What about error level analysis? The brightness thing.



Herman

FotoForensics says it themselves, it's a lead, not proof. High contrast edges glow naturally, and re-saving a file can hide a genuine edit. And no pixel test at all can see what happened before the shutter. The point keeps coming back the same way: detection is an arms race you lose slowly. Provenance at capture is the thing that actually gets stronger over time.



Corn

There's one more problem, and it's my phone. It's been editing my photos without asking for years.



Herman

It has, and this one is genuinely awkward for "unaltered". Samsung's moon business, where a blurry moon on a monitor came back with craters the camera never saw. Google's Best Take, which builds a group photo out of faces from several frames. Add Me, which merges people from separate shots. None of that is evil, but if you're shooting evidence, turn off the scene enhancement, shoot in the plain photo mode, leave the AI tools alone, and if your phone offers a raw format, a second copy in raw doesn't hurt.



Corn

Don't touch the file afterwards either. No crop, no brighten.



Herman

Don't touch the original, ever. If you need a cropped version for a letter, make a copy and say it's a copy. And keep the originals properly. Google Photos takeout is a trap here, it pulls metadata out into a separate side file, and edited versions come back with "edited" in the name. People then merge the metadata back in with a tool and occasionally overwrite real location data with zeros.



Corn

Where does the original go, then?



Herman

Off the phone, as the actual original file, to two places. A cloud folder with its own upload dates, and one more you control. Then the hash in an email to the other party. If you want to be thorough, there are timestamping services. The formal standard is RFC thirty-one sixty-one, where an authority signs your hash with the time. Or OpenTimestamps, which anchors your hash in the Bitcoin blockchain, so anyone can check it later without trusting any company at all.



Corn

Bitcoin finally does something useful, and it's to win my deposit back.



Herman

In the EU there's a formal tier, qualified timestamps under their e-signature regulation, which carry a legal presumption. Blockchain ones don't get that. I wouldn't lose sleep over it for a deposit. The other party's inbox is doing most of the work, frankly. Shelter, the English housing charity, says to film on the day you move out, attend the checkout, and compare against the move-in inventory line by line. Glossy photo-only inventories are weak. Words next to pictures.



Corn

I'll say what I think is the strongest thing a tenant can have. A move-in video and a move-out video, shot the same...



Hilbert

...route. Same doorway first. Same order through the rooms. I call it the lap. If the two laps run the same way you can play them side by side and it does the arguing for you.



Herman

That's a better point than mine was going to be.



Hilbert

I'm doing one Tuesday. A man called Gideon Asaf. Eleven years in a flat on Shmuel Hanavi. He wants his deposit back. The landlord says the flat had a parquet floor. It never had a parquet floor. Nobody in the building has ever seen parquet.



Corn

And he has the move-in lap.



Hilbert

He has a move-in lap. Six minutes. He shot it on a phone that opened like a clam. It goes front door, kitchen, hall, bedroom, and then for the last two minutes it's his shoe, because he answered a call and kept filming. The shoe is very clear. You can read the size.



Herman

Even the shoe helps, honestly. Unbroken take, no cuts. If the floor's visible in any of it...



Hilbert

The floor is visible under the shoe. Tiles. Terrazzo. Forty centimetre squares, you can count them. So the lap Tuesday follows his lap to the step. Front door, kitchen, hall, bedroom, then I film his shoe for two minutes. Same shoe. He still has it. He kept the pair because the left one was the evidence.



Corn

That's the first sensible thing anyone's done with a shoe.



Hilbert

The difficulty is the bathroom. The landlord sublets the bathroom. Separately. To a dentist. Dr. Ronit Halabi. She sees patients in it on Tuesdays and Thursdays. There's a chair. It reclines. Gideon has had to shower at his sister's in Talpiot for about four years. He says he doesn't mind, the water pressure is better.



Herman

The bathroom's in the lap, then, but it isn't technically his.



Hilbert

It was his on move-in. It's on the six minutes. So it has to be on Tuesday's lap or the laps don't match. I booked Gideon a cleaning. Twelve fifteen. That puts him in the chair, in the room, with a witness who has a professional licence. And the patients in the waiting area, which is the hallway, become witnesses to the hallway. I've printed consent forms. Two hundred and ten. I don't know how many patients she sees. I rounded up.



Corn

You've thought harder about this than his lawyer.



Hilbert

He hasn't got a lawyer, Corn. He's got me and a broom handle. I priced a gimbal for it, at the place on Agripas. Six hundred and forty shekels. I'm taping the phone to the broom instead. Herman, you said hash about forty times this morning. I'll be doing the hash. I'll do it on his sister's laptop, because she's the one with the laptop and she's the only one the landlord's still speaking to.



Herman

Then email it to the landlord the same afternoon, and the lap is in his inbox with his own server's date on it.



Hilbert

That's the plan. The landlord has asked if he can narrate. I've said yes. He wants to do the kitchen. He's very good on kitchens. He used to be a weatherman on local cable, and he describes cupboards like a front coming in off the coast.



Herman

He's narrating his own evidence against himself.



Hilbert

He thinks it'll help him. He's going to point out the parquet. Gideon's move-in lap from eleven years ago runs six minutes and eight seconds. Tuesday's has to run six minutes and eight seconds too, or he says it doesn't count. Dr. Halabi's appointments are twenty minutes. I've told her the cleaning has to finish at twelve twenty-one and fourteen seconds.



Corn

The laps having to match is the part I'd actually steal. Not the dentist.



Herman

It's the part most tenants miss. People shoot move-in carefully and then move-out in a panic on the last day, in a different order, half the rooms already full of boxes. The two videos don't line up, so nobody can compare them, and an argument nobody can compare goes to whoever sounds surer.



Corn

Which is usually the landlord. Daniel, if you do one thing differently, plan the move-out lap on the day you shoot the move-in one. Same route, same order, same narration, wide then close. The tools sit on top of that. Timemark's code for an independent server record, ProofMode or a Pixel's native credentials for a signed fingerprint, and the files sent as files to the other party the same day.



Herman

Keep the original that's never been through a messaging app. Every one of those protections dies the first time the video gets compressed, and nothing warns you when it happens.



Corn

What I'm curious about is whether the lap stops being a tenant's trick and becomes the norm. Apple's signing what hits the sensor, Sony's checking for depth, the rules committees are still arguing. But the thing that would have settled the Alameda case is boring. Two videos of the same flat, same route, years apart, one in each party's inbox.



Herman

The cryptography only ever proves the file's still the file. The rest is somebody walking the same hallway twice.



Corn

Thanks as ever to our producer Hilbert Flumingtop, who keeps this thing on air.



Herman

This has been My Weird Prompts. If you want the back catalogue, it's all at my weird prompts dot com.



Corn

See you tomorrow.