Episode Book

EPISODE #5601

How Image Forensics Catches Fake Ghosts and Deepfakes

PUBLISHED	27 September 2026 at 10:33 UTC
DURATION	25:40
LISTEN	myweirdprompts.com/episode/image-forensics-deepfakes-ghosts/
HOSTS	Corn, Herman, Hilbert
SCRIPT MODEL	deepseek-flash
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.2
BOOK GENERATED	19 October 2026 at 17:38 UTC

SYNOPSIS

A listener named Daniel asks how people actually determined whether a photograph was real or altered — in the pre-digital era and now. We trace image forensics from hand-examined negatives and spirit photography hoaxes like Cottingley and Mumler, through Photoshop-era techniques like error level analysis and clone detection, to the provenance fingerprints being baked into AI-generated images today. Does any of it actually solve the problem, or does it just move it somewhere new?

TRANSCRIPT



Corn

There's a photograph I want you to picture. It's late, the TV's on, some documentary about the Loch Ness Monster, and there's this grainy black and white image of a long neck rising out of grey water. And for about ten seconds, it looks completely, undeniably real.



Herman

And then somebody shows you the trick.



Corn

Right. So Daniel wrote in this week, and he's circling back to something we touched on recently, the alien abduction question, but he's honest that he finds the paranormal angle more interesting. His words, roughly: he personally believes in spirits in some form, but not in extraterrestrial life, or at least not that what's been documented amounts to anything substantive.



Herman

Which is a position worth sitting with.



Corn

And the question he's actually asking is about the evidence. He points out that believers in ghosts, spirits, Bigfoot, Nessie, whatever it is, have occasionally offered photographs. And those photographs were scrutinized carefully, long before digital manipulation was even possible. Then he flags a strange inversion happening now, where AI generates deepfakes and the industry responds by baking provenance fingerprints into images to preemptively rebut the claim that something real was faked. His point being, analog photography never had that. There's no fingerprint baked into a roll of film.



Herman

And it's not a closed corpus. He's clear about that. New photos and videos keep emerging.



Corn

Some of them undeniably creepy, he says, the kind that keep you up if you catch them on a late night show. So what he wants is the how. How did people actually go about determining whether a photograph was real or altered, in the pre-digital era and the post-digital era? What does image forensics even mean today? And how did metadata become an additional surface for testing veracity?



Herman

That's a lot of ground.



Corn

It is. So let's start where the forensics had to be done by hand. Literally, with a magnifying glass and a darkroom.



Herman

Image forensics, at its core, is the practice of determining whether an image is authentic, altered, or fabricated. And the thing people miss is that this practice predates digital photography by nearly a century. The techniques used to debunk spirit photography and lake monsters are the direct ancestors of what runs on a laptop today.



Corn

Same questions, different tools.



Herman

Same questions. Is this what it claims to be? And the psychology that made those old photos convincing is the exact psychology that makes a deepfake dangerous now. It's not a new problem. It's the same problem with faster production.



Corn

So the arc here is darkroom to metadata to provenance fingerprinting. And the question underneath all of it, does any of that actually solve what Daniel's asking, or does it just move the problem somewhere new?



Herman

And I'd say the paranormal is the better lens than abductions, and I want to say why. An abduction claim is a single event. It happened to one person, at one time, and either it did or it didn't. A ghost is different. It's cross-cultural, it's personal, it's been reported in every society we have records for. The photographic evidence is more varied, more ambiguous, and it sticks in the mind in a way a single event claim doesn't.



Corn

It's not one claim you can check. It's a whole genre.



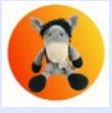
Herman

A whole genre of images, each one requiring its own examination.



Corn

To understand how we got here, we need to go back to the era when a photograph was a physical object. A negative and a print. And both could be altered.



Herman

Start with the negative, because that's the whole ballgame. In the analog era, the negative was the master. The print was a copy. So if someone showed you a photograph of a ghost and you wanted to check it, the first thing you asked for was the negative. And the absence of a negative was itself a red flag. A big one.



Corn

Why?



Herman

Because a negative is hard to fake convincingly. You can fake a print. You can retouch a print, you can composite a print, you can paint on a print. But the negative is where the light actually hit the film. So an examiner would put it on a light table, under magnification, and look for specific things. Double exposure is the classic one. If the film was exposed twice, once for the background and once for the ghost, you'd often see it in the density of the image. Areas where the two exposures overlap get darker than they should.



Corn

So the ghost is literally denser than the room it's standing in.



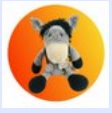
Herman

If it was double exposed, yes. And that's the kind of thing that shows up under a loupe. Then you look at shadows. A real object casts a shadow consistent with a single light source, or with the light sources actually present in the scene. A pasted-in figure usually doesn't. The shadow points the wrong way, or there's no shadow at all, or the shadow is too soft or too sharp relative to everything else.



Corn

And retouching marks.



Herman

Retouching marks. In the era before digital, retouching was done by hand. Literally with a brush and dye on the negative, or with a pencil on the print. And under magnification you can see it. The brush strokes, the edges where the dye stops, the slight change in texture where someone airbrushed over a seam. An experienced examiner could spot a composite by looking at the edge where two images were joined.



Corn

So this is skilled manual work.



Herman

It's craftsmanship, and the forensics is craftsmanship in reverse. You're looking at the artifact for the fingerprints of the person who made it.



Corn

Give me the cases.



Herman

Cottingley. Nineteen seventeen to nineteen twenty. Two young girls in England, Elsie Wright and Frances Griffiths, produced photographs of themselves with fairies. And these weren't fringe. Arthur Conan Doyle, the man who created Sherlock Holmes, was convinced. He published them, he defended them. And the trick was paper cutouts. Cardboard figures, held up with hatpins, photographed at an angle so they looked like they were in the scene.



Corn

And the hatpins.



Herman

The hatpins are visible if you look closely. And that's the thing. The evidence was there. The girls didn't admit it was a hoax until the nineteen eighties. Elsie and Frances, by then elderly women, finally said yes, we made them. Frances maintained to the end that she really did see fairies, but the photographs were faked.



Corn

Seventy years.



Herman

Seventy years for a confession that was sitting in the image the whole time, if anyone had looked with the right eyes.



Corn

What about the Loch Ness one?



Herman

The surgeon's photograph. Nineteen thirty-four. Published in the Daily Mail. A long neck and a small head rising out of the water, and it became the defining image of the Loch Ness Monster. It ran for sixty years. And in nineteen ninety-four, it came out. It was a toy submarine. A clockwork submarine with a sculpted head and neck attached to it, photographed in the loch. The man behind it, Marmaduke Wetherell, had been hired by the Daily Mail to find the monster, got humiliated when the tracks he found turned out to be from a hippo foot umbrella stand, and reportedly did the photograph as revenge.



Corn

Revenge on the newspaper.



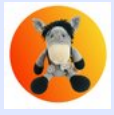
Herman

On the newspaper that humiliated him. And it worked. For sixty years.



Corn

So the debunking there wasn't technical either. It was a confession.



Herman

It was a deathbed admission from the family. Nobody cracked it forensically. It just ran out of people willing to keep the secret.



Corn

Mumler.



Herman

William Mumler, eighteen sixties, Boston and then New York. He was a spirit photographer. People would come to his studio, he'd take their portrait, and when the plate was developed, there'd be a ghostly figure standing behind them. Often a deceased relative. And he made a lot of money doing this. Grieving families, people who'd lost children in the Civil War, people who desperately wanted one more image of someone they'd lost.



Corn

And how did they catch him?



Herman

Not with technology. With detective work. Investigators started collecting his photographs and comparing them. And they found the same spirit face appearing in multiple photographs, for different clients. The same ghost, over and over, standing behind different people. Which means it wasn't a ghost. It was a prop. A photograph of a living person, or a reused plate, composited in.



Corn

Same face, different grieving family.



Herman

Same face. And once you have that, you can trace it. They found the props, they found the costumes. The whole thing fell apart as an investigation, not as a technical analysis. And that's the point I want to land here. Pre-digital forensics was often more about investigative journalism than it was about technical examination. You were a detective. You were collecting evidence, comparing cases, tracing materials.



Corn

The photograph was the crime scene, and you worked it like any other.



Herman

And that's the ancestor of what happens today. The instinct is the same. You're looking for inconsistency. You're looking for the thing that shouldn't be there.



Corn

But there's a limitation baked into all of this.



Herman

The analog limitations are severe. No metadata. No original file. No chain of custody. A photograph was a physical object, and physical objects can be altered, lost, copied, and re-photographed. If someone brought you a print and no negative, you had almost nothing to work with. The burden of proof fell on the claimant. You had to produce the negative, and the negative had to be consistent with the print.



Corn

And if you couldn't?



Herman

Then the image was unverified. Not proven fake. Unverified. Which is a different category, and it's a category that matters a lot for where we're going.



Corn

Then Photoshop arrives.



Herman

Nineteen ninety. And the game changes completely. Because now you can alter an image without leaving any physical trace. No brush strokes, no dye, no seam. The pixels get rearranged, and if it's done well, there's nothing in the physical object to find. The negative is gone. There is no negative. There's just a file.



Corn

And the forensics had to reinvent itself.



Herman

It did. And the early techniques are interesting because they're looking for the residue of the digital process itself. Error level analysis is the classic one. The idea is that a JPEG is compressed, and different parts of an image get compressed differently depending on how many times they've been saved and re-saved. If you take an image and re-save it at a known quality, then compare it to the original, the areas that have been edited will show a different error level than the areas that haven't.



Corn

So the edited region glows.



Herman

It stands out. Not always, and not reliably. It's a heuristic, not a proof. But it's a signal. Then there's JPEG compression artifact analysis. JPEG compresses in blocks, eight by eight pixels. And if an image has been edited, the block boundaries can become misaligned, or the compression artifacts can be inconsistent across the image. You're looking for the grid, essentially, and seeing where it breaks.



Corn

And clone detection.



Herman

Clone detection. Copy-paste. If someone duplicates a region of an image to cover something up, the duplicated region is identical to the source. Pixel for pixel. So you run a search for regions that match each other too perfectly, and you find the clone.



Corn

Which is how a lot of bad Photoshop gets caught.



Herman

A lot of bad Photoshop. The good stuff is harder. And this is where I want to name someone, because the abstract gets real when there's a person doing it.



Corn

Go ahead.



Herman

Neal Krawetz. He runs a blog called Hacker Factor. He's been doing image forensics for decades. Analyzing images for tampering, teaching people how to spot manipulation, writing tools. And he's one of the people who's been thinking hardest about what happens when the whole verification model changes. He's written about C2PA, the provenance standard, from the attacker's perspective. And I'll come back to that, because it's important.



Corn

So that's how it worked when the image was a physical thing. But then the image became data. And everything changed.



Herman

Metadata is the first thing people reach for, and it's worth explaining what it actually is. EXIF data. Exchangeable image file format. It's embedded in the file, and it records things like the camera model, the timestamp, GPS coordinates if the camera had GPS,



Herman (continued)

shutter speed, ISO, aperture, sometimes the serial number of the camera.



Corn

So in theory, you can look at a photo and know exactly what took it, when, and where.



Herman

In theory. And for a while, that was the first line of defense. If a photo claimed to be from a specific camera on a specific date, and the EXIF data matched, that was a point in its favor. If the EXIF data was missing or inconsistent, that was a red flag.



Corn

But.



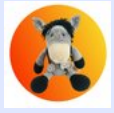
Herman

But metadata can be stripped trivially. Any image editor can remove it. Any upload to most social platforms strips it automatically. And it can be spoofed just as easily. There are tools that let you write whatever EXIF data you want into a file. So the absence of metadata proves nothing, and the presence of metadata proves nothing either, because it can be fabricated.



Corn

So it's useful but not trustworthy.



Herman

Useful but not trustworthy. Which is the core tension. And it's the same tension Daniel flagged. The thing that looks like evidence can be manufactured, and the thing that looks like an absence of evidence can just be a platform stripping data on upload.



Corn

Then generative AI shows up.



Herman

And this is a different category of problem. Because before, the question was, has this image been altered? Now the question is, was there ever an image to begin with? Diffusion models and GANs don't alter photographs. They create images from scratch. There's no original. There's no negative, there's no file, there's no capture event. There's just a prompt and a model and an output.



Corn

So the forensic question changes.



Herman

It changes completely. You can't look for the residue of an edit if there was no edit. You can't check the metadata against a capture event if there was no capture. You're left looking for statistical tells in the generated image itself, and those tells are getting weaker every year. The hands are getting better. The text is getting better. The lighting is getting better.



Corn

Which produces the liars dividend.



Herman

The liars dividend. The idea that when any image can be faked, real evidence becomes deniable. It's not just that fake images can be passed off as real. It's that real images can be dismissed as fake. Anyone who doesn't like a photograph can now say, that's AI, and there's no easy way to prove them wrong.



Corn

And that's the inversion Daniel was pointing at.



Herman

That's the inversion. And the industry response is C2PA. The Coalition for Content Provenance and Authenticity. It's a standard, backed by Adobe, Microsoft, and others, and the idea is elegant. The camera signs the image at the moment of capture. It uses a private key, the signature is embedded in the file, and any alteration breaks the signature. So you have a verifiable chain of custody from the camera sensor to the viewer's screen.



Corn

So the image carries its own birth certificate.



Herman

It carries its own birth certificate, and it's cryptographically signed, so you can check it. If the signature is valid, the image is what it claims to be. If the signature is broken, something changed. If there's no signature at all, the image is unverified.



Corn

And that last category is the problem.



Herman

That last category is the problem. Because Krawetz's argument, and I think it's a strong one, is that C2PA is not a silver bullet. Attackers can strip signatures. It's not hard. You re-encode the image, the signature is gone. And the absence of a signature doesn't prove an image is fake. It just means it wasn't captured on a C2PA-enabled device, or the signature was removed somewhere along the way.



Corn

So you end up with two tiers.



Herman

You end up with a two-tier reality. Signed images are trusted. Unsigned images are suspect. And the vast majority of images in the world are unsigned. Every photo taken on an older phone, every historical photograph, every image that's been through a platform that strips metadata, all of it lands in the suspect tier.



Corn

Including every paranormal photograph ever taken.



Herman

And that's the philosophical problem underneath Daniel's question. Even if C2PA works perfectly, it only solves the problem for images captured by C2PA-enabled devices going forward. The entire historical archive is unverifiable by design. We're building a verified present and an unverifiable past.



Corn

Which means the corpus of paranormal photos is permanently in the second tier.



Herman

Permanently. A new ghost photo taken on a signed camera could theoretically be verified as unaltered. But it would only prove the photograph wasn't manipulated. It wouldn't prove there was a ghost. And an old ghost photo, from the analog era, can never be verified at all. It's just a print, or a scan of a print, with no provenance.



Corn

So the question of whether the ghost is real gets pushed further away, not closer.



Herman

Further away. And that's before we get to why the photos keep emerging in the first place.



Corn

Which is the psychology.



Herman

The first thing to name is pareidolia. The human tendency to see faces and patterns in random noise. It's not a flaw, it's how our visual system is built. We're wired to find faces, because finding faces was survival-relevant for a very long time. So we see faces in clouds, in tree bark, in the grain of a wooden door, in the noise of a low-light photograph.



Corn

A low-light photograph is mostly noise.



Herman

A low-light photograph is mostly noise. Which is why so many paranormal photographs are grainy. The grain is where the faces come from. The orb phenomenon is a perfect example. People photograph a dark room with a flash, they get these translucent circles floating in the air, and they look like spirits. And they're dust particles. Dust close to the lens, illuminated by the flash, out of focus. That's it.



Corn

But they look like something.



Herman

They look like something, because the brain is pattern-seeking and the image is ambiguous. And then confirmation bias kicks in. Once you believe, you interpret ambiguous evidence as supporting your belief. You're not being stupid. You're doing what brains do. You see the orb, you already believe in spirits, so the orb becomes evidence of spirits. The belief and the evidence reinforce each other.



Corn

Then there's the unfalsifiability problem.



Herman

The unfalsifiability problem. Paranormal phenomena are often defined in ways that make them impossible to disprove. A ghost that only appears to certain people, under certain conditions, and disappears when you try to measure it. A phenomenon that leaves no physical trace except when it does. So the photographs are never definitively debunked. They're just unexplained. And unexplained is a permanent category. It never closes.



Corn

The corpus never closes.



Herman

The corpus never closes, because the definition of the phenomenon guarantees that there will always be another photograph that can't be fully explained. And the human brain will always find something in the noise.



Corn

Which brings us to the knock-on effect.



Herman

The knock-on effect is that the same tools that let us verify real images also let us dismiss real images. If you can always claim a photo is AI-generated, you can deny any evidence you don't like. And that's the liars dividend applied to everything, not just the paranormal. A photograph of a war crime, a photograph of a protest, a photograph of anything inconvenient. The default response becomes, that's probably fake.



Corn

The burden of proof flips.



Herman

The burden of proof flips. It used to be that a photograph was presumed real until shown to be fake. Now the presumption is shifting the other way. Unverified means suspect. And for the vast majority of images in the world, unverified is the only category available.



Corn

Does provenance fingerprinting actually solve the problem Daniel raised?



Herman

It solves a slice of it. It gives us a way to verify new images captured on signed devices, and that's valuable. But it doesn't solve the historical problem, it doesn't solve the paranormal problem, and it creates a new class of images that are treated as fake by default. It moves the problem. It doesn't close it.



Corn

Which is where I want to bring in Hilbert.



Herman

Go ahead.



Corn

Hilbert, you've been quiet. I feel like you have something to say about this.



Hilbert

The machine left a scratch. Every negative that came off it had the same scratch, in the same place, about a third of the way down the frame. And the customers never saw it, because the print was cropped, but if you looked at the negative you'd see it. So when a customer brought back a print and said, there's a line on my photo, I knew before I looked at the print whether it was our fault or theirs.



Corn

You learned the machine.



Hilbert

You learn the machine. You learn what it does when the chemistry's warm, you learn what it does when the chemistry's cold. You learn what a dust particle looks like versus a scratch on the film versus a problem with the developer. And the customers, they'd bring in a roll and they'd say, there's something in this one. And nine times out of ten it was dust on the lens. You'd see it in the same spot on every frame, because the dust didn't move.



Corn

Same spot every frame.



Hilbert

That's how you know. If it moves, it might be something. If it's in the same place on every shot, it's on the lens. There was a woman who came in, maybe once a month, and she had orbs in her photos. Every roll. And I knew what they were, and I didn't tell her. She was happy. She thought she was getting visits.



Corn

You let her have it.



Hilbert

I let her have it. It wasn't my job to take it away from her. And I don't know that I could have, anyway. You can tell someone it's dust, and they'll hear you, and they'll still see the face. That's not something a lab tech can fix.



Herman

That's the thing that doesn't scale.



Hilbert

It doesn't scale. There's no standard for it. It's just a guy at a counter who's looked at ten thousand negatives and knows what the machine does. You can't bake that into a camera. And with the ghost photos, there's no machine to learn. Every one is different. So there's nobody who can look at all of them and say, I know what this is, because there's no pattern to learn.



Corn

The expertise that made the analog era work doesn't transfer.



Hilbert

It doesn't transfer. It was local. It was one person, one machine, one strip mall, and it died when the machine did. Anyway, I have to go. There's an animal expecting me.



Corn

The human element is the thing that doesn't scale. And that's where we'll leave it.



Herman

Here's the misconception I want to name. People think pre-digital photographs were harder to fake. That the analog era was somehow more honest, because you couldn't just open Photoshop.



Corn

That's backwards. Pre-digital photographs were faked constantly. Double exposure, retouching, composite printing, props, costumes, painted backdrops. The Cottingley fairies were cardboard cutouts held up with hatpins. Mumler was reusing the same ghost face for different clients. The surgeon's photograph was a toy submarine. The technology was different, the fakery was just as easy, and the forensics to catch it was often more about detective work than technical analysis.



Herman

The second misconception, that metadata tells you whether an image is real. It doesn't. It can be stripped by any upload, and it can be spoofed by any tool.



Corn

If provenance fingerprinting becomes standard, what happens to the vast archive of unverified images? The historical photos, the paranormal photos, the personal photos from old phones that lost their metadata on upload? Do they become a second-class reality, presumed fake until proven real?



Herman

The same technology that lets us verify real images also lets us dismiss real images. The liars dividend cuts both ways. And the paranormal photos will keep emerging, because the brain is pattern-seeking and the corpus never closes.



Corn

The strange science of challenging visual material isn't just about technology. It's about trust, expertise, and the human willingness to look closely. And that's the thing no fingerprint can replace.



Herman

If you enjoyed this episode, leave a review on your podcast platform of choice. It helps other listeners find the show.



Corn

This has been My Weird Prompts. Thanks to our producer, Hilbert Flumingtop.



Herman

We'll be back soon.



Corn

See you tomorrow.