Episode Book

EPISODE #6144

8 Real Steganography Cases and How They Got Caught

PUBLISHED	19 October 2026 at 19:27 UTC
DURATION	25:57
LISTEN	myweirdprompts.com/episode/real-steganography-cases-caught-88408/
HOSTS	Corn, Herman, Larry, Hilbert
SCRIPT MODEL	anthropic/claude-haiku-5.5
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.10
BOOK GENERATED	20 October 2026 at 07:46 UTC

SYNOPSIS

In 2002, USA Today reported that al-Qaeda was hiding encrypted messages inside eBay images. Two University of Michigan researchers scanned two million eBay pictures and found nothing — and that gap between headline and evidence is where this episode begins. We count down eight documented cases of steganography actually used in the wild, from a World War I null cipher that spelled out Pershing's sailing date in the first letter of every word, to a Manhattan doll shop whose letters described warships as dolls, to a Navy pilot who blinked TORTURE in Morse code during a televised 1966 interview. The through-line is startling: almost none of these messages were caught by the hidden payload itself. A caption, an envelope, a run of hotel typewriters, a microphone — something else always gave it away. We dig into what each case reveals about how real covert communication succeeds, why dull covers beat clever ones, and why a clean scan of two million images proves less than it seems.

TRANSCRIPT



Corn

Here's the picture you've probably got in your head. Terrorists hiding their plans inside pictures on eBay, and nobody can see a thing. Herman, that's the story, isn't it?



Herman

That's the story, and it's a good one, which is the trouble. In February two thousand one, USA Today reported that encrypted attack plans might be hidden in pictures on porn sites and in sports chat posts. Then in July two thousand two, the same paper wrote that al-Qaeda had sent hundreds of encrypted messages hidden in files on eBay.



Corn

And eBay said what?



Herman

eBay said nobody from the federal government had contacted them. That was the whole response.



Corn

So a secret message went through the one company that would have to know about it, and the company had never heard of it.



Herman

Which should have been the end of it. But somebody did go looking, and I love that part. Two researchers at the University of Michigan, Niels Provos and Peter Honeyman, scanned about two million eBay images in two thousand one, using tools that look for the known hiding programs. They found no hidden messages at all.



Corn

Two million pictures of other people's used things, and nothing in any of them.



Herman

Provos was careful about what that meant, and he should have been. He said, "I can't answer the question of whether or not there is hidden content on the Internet." A clean scan only tells you about the programs your scanner already knows. Anything built differently walks straight past it.



Corn

So it's a clean result on a narrow question, sitting under a headline with no narrow question at all.



Herman

There's the other side too. A company called WetStone said it had found hidden messages on eBay and Amazon. Its Chet Hosmer later put a rough number on it: about one picture in a hundred thousand looks suspicious. That's a long way from a picture that carries a message. Salon did the arithmetic at the time. To find a hundred real messages you'd have to scan somewhere between one and two billion images, which is more than eBay had listed since the attacks.



Corn

So the most famous steganography case in the world is a scare with no sample behind it. Good. That's the warm-up.



Herman

Daniel's question is about the real ones. The weirdest documented cases of steganography actually used in the wild, with the messages that were hidden, and how each one got caught. So let's count them down, eight to one. And I'll give away the through-line now. Almost none of them were caught by the hidden message itself.



Corn

Something else always gave it away. A caption, an envelope, a scrap of paper, a microphone. Never the message.



Herman

Number eight is the oldest, and the simplest. It's called a null cipher. The real message sits in the first letter of every word, and the rest of the text is ordinary wording that happens to read as a sentence. In the First World War, a German message went like this, in full: President's embargo ruling should have immediate notice. Grave situation affecting international law. Statement foreshadows ruin of many neutrals. Yellow journals unifying national excitement immensely.



Corn

That's a complaint about an embargo, written by a man who has been asked for a sympathy card.



Herman

Now take the first letter of each word. Pershing sails from New York, June the first.



Corn

So the payload is a sailing date for John Pershing, the American commander, tucked inside a grumble about trade rules.



Herman

Pershing commanded the American forces in France, yes. And the sailing date is the whole point of the thing. Think about who was reading. In that war, cables were read by censors, so the cover had to survive a censor, and a grumble about trade rules is just what a censor waves through. Hiding the date was easy, because the cover only has to be grammatical. The trick is that the sentence has to be dull enough that nobody reads past the first word of each line. David Kahn's history of codebreaking uses it as the textbook example.



Corn

Dull is doing a lot of work in that sentence.



Herman

It's doing all of it. Corn, would you have spotted that?



Corn

Only if somebody had told me to count the first letters.



Herman

That's the hard part, and it's the same for every case on this list. The record doesn't tell us who the message was going to, or how it got past anybody, and I'm not going to guess. What I can say is that a null cipher only works once you know to look for it. The cover is the lock, and the first letters are the key.



Corn

Number seven. The doll woman.



Herman

Velvalee Dickinson ran a doll shop in Manhattan, at seven hundred and eighteen Madison Avenue. That address is a Beretta gallery now. In January nineteen forty-two, a letter went out from Springfield, Ohio, signed by a woman calling herself Mary Wallace, and addressed to a Señora Inez Lopez de Molinali in Buenos Aires. It read: The only three dolls I have are three love Irish dolls. One of these dolls is an old fisherman with a net over his back, another is an old woman with wood on her back and a third is a little boy.



Corn

Three love Irish dolls. Nobody in the doll trade has ever stocked that.



Herman

The FBI read it, and read it well. The fisherman with a net over his back was an aircraft carrier, sitting behind an anti-submarine net. The old woman with wood on her back was a battleship with a wooden deck. The little boy was a destroyer. There were five letters like it, between January and August of nineteen forty-two, each one describing warships in the language of a shop.



Corn

So a battleship is an old woman with wood on her back. The Navy is not going to like that.



Herman

Why spread them out, though? My guess is that you don't send five letters in one bundle, because one bundle is one thing to catch. Spread them over eight months and each one is a small, dull piece of correspondence from a doll shop.



Corn

A doll shop with a steady trade in navies.



Herman

The letters didn't do her much good, in the end. The Japanese had quietly shut down the Buenos Aires drop address, so the mail came back undelivered. It's the only spy network I know where the post office closing down is the main plot point.



Corn

The spy post office was closed, and she kept posting letters to it.



Herman

And the people who caught her weren't mainly reading the doll descriptions. The signatures on the letters were the names of real doll collectors, who said they hadn't written them, and every one of those collectors knew Dickinson. The typing analysis tied the letters to one typist, using a run of different hotel typewriters. And the codebreaker



Herman (continued)

Elizebeth Friedman noticed that the return address changed on every envelope. Her reading was that the letters were meant to be intercepted, and that's the reading that stuck.



Corn

So the one careful thing she did was make sure somebody opened the envelope.



Herman

Yes. The careful part was the cover. She had a real shop, selling real dolls, run by a real woman, and the strange language only ever appeared on the page.



Corn

A real doll shop with real dolls. That was the whole disguise.



Herman

She was arrested in January nineteen forty-four, at a bank in Midtown, and fifteen thousand nine hundred and forty dollars was sitting in her safe deposit box. She pleaded guilty to censorship charges and got ten years. And the judge refused to let her take her record player to jail, which is in the record, and which I think is the single most human detail in the whole episode.



Corn

Good for the judge.



Herman

Strictly speaking, I should say this isn't steganography. The FBI called it an open code. You can read every word of the letters, and the Navy is right there in the sentence. But it's the same instinct as the hidden ones: a cover that's more interesting than the plain letter, sent somewhere nobody checks.



Corn

Six already. Go on.



Herman

Number six. Jeremiah Denton, and a blink. Hanoi, nineteen sixty-six. Denton was a Navy pilot held as a prisoner of war, and he sat for a televised interview with a Japanese reporter. The captors wanted the film for propaganda, and they got some. Under a pretext about being sensitive to the lights, Denton blinked out the letters T, O, R, T, U, R, E in Morse code. The word is torture. Later he became a United States senator from Alabama, which is a strange career path for a man who once spelled out that word for a camera.



Corn

The camera was watching his mouth. He was talking with his eyes.



Herman

On camera he said, I get adequate food and adequate clothing and medical care when I require it. And then: I don't know what is happening, but whatever the position of my government is, I support it, fully.



Corn

Adequate food, adequate clothing, and then a blink that spells torture. That's a man reading the script he was given, with his eyes.



Herman

Naval Intelligence reviewed the tape, and it was the first clear confirmation that American prisoners were being tortured. That's a lot to have come out of a blink. The tape is now in the CIA's collection at the National Archives. Denton later guessed the captors didn't learn what he'd spelled until nineteen seventy-four. So for eight years the message sat in the film, and the people who made the film didn't know it was there.



Corn

The captors got the eyes wrong, and the people who caught it were the ones who sat down with the tape afterwards.



Herman

Corn, would you have caught it live?



Corn

If somebody had told me to watch his eyes, yes. I'd have been watching the reporter.



Herman

Fair. Everybody in that room was watching the reporter.

L

Larry

Tired of nosy governments reading your holiday photos? Tired of your private messages being read by people who have no business reading them? Then you need Pillow Pixel Deluxe, the only null cipher you can sleep on. Write your secret in the first letter of every word, tuck it inside the sky of any photo you take on your phone, and nobody will ever look at a sunset and think, that's a null cipher. Pillow Pixel Deluxe is endorsed by no authority, tested by no laboratory and used by no government, which is exactly why it is safe. It works on dogs. It works on your grandmother's sofa. It works in the rain, on the balcony and on the stairs.



Corn

Tired of nosy governments reading your holiday photos.

L

Larry

Now only four hundred shekels! Four hundred! And as a thank you, we are throwing in a cuckoo clock, a bag of walnuts, a lifetime subscription to a man called Gary, and a bicycle lock, which you will not need, but it is yours. Now three hundred. Now two hundred and ninety, and the walnuts are free, and the sofa comes in a second color, and forty-one hats

L

Larry (continued)

are included, the hats are not optional, the hats are the offer, and the offer ends right now, which is



Herman

Corn, please don't do that again.



Corn

Number five. The Pueblo, nineteen sixty-eight.



Herman

The USS Pueblo was a Navy intelligence ship, and North Korea seized it. The crew had prepared for the worst, and part of the preparation was a cover story for the photographs. When the cameras came out, the crew gave the middle finger, and told the captors it was a Hawaiian good luck sign. The crew called the whole thing The Digit Affair. Stu Russell, one of the men on board, put it plainly: the finger became an integral part of our anti-propaganda campaign. Any time a camera appeared, so did the fingers.



Corn

Would you have made that gesture with a camera pointed at you?



Herman

Probably not, and I'd like to think I'd have found something else. But they were in a situation with nothing to do but find things, and the finger didn't need anything except a hand.



Corn

A Hawaiian good luck sign. Who was going to check?



Herman

The captors checked, for a while. Then in October nineteen sixty-eight, Time ran a photo, and the caption explained the gesture to everybody. The caption said three of the crewmen had managed to use the medium for a message, furtively getting off the United States hand signal of obscene derisiveness and contempt.



Corn

So the message got through perfectly well. Then the caption told the whole world what it said.



Herman

And the crew paid for it. What followed, the crew themselves called Hell Week. Beatings. They were held for three hundred and thirty-five days, and released on the twenty-third of December, nineteen sixty-eight.



Corn

The good luck sign was a perfectly good cover, right up until the magazine explained it.



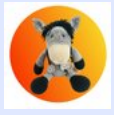
Herman

That's the pattern, Corn. The cover held. The leak came from the print run.



Corn

Number four. The illegals. Their pictures were better than the sofa.



Herman

June twenty ten, the FBI arrested a group of Russian agents who had been living as ordinary Americans, in ordinary houses, for years. They had a steganography program that Moscow Centre supplied, not on sale anywhere, and it hid text inside ordinary photographs. The FBI's complaint says: These images appear wholly unremarkable to the naked eye. But these images, and others, have been analyzed using the steganography program. As a result of this analysis, some of the images have been revealed as



Herman (continued)

containing readable text files.



Corn

Wholly unremarkable. Every holiday album in the country would frame that review.



Herman

The software worked at the level of single pixels, the red, green and blue values of each dot, which is why a picture can look the same to you and still carry a file.



Corn

So the picture is a suitcase with no visible zip.



Herman

And the content is worth hearing. A message from Moscow in two thousand nine, decrypted, addressed to a couple using the names Richard and Cynthia Murphy, reads: You were sent to USA for long-term service trip. Your education, bank accounts, car, house, et cetera, all these serve one goal: fulfill your main mission. That is, to search and develop ties in policymaking circles in US, and send intels, meaning intelligence reports, to Center.



Corn

Long-term service trip. Sounds like a holiday with a mortgage.



Herman

Which is about right. They'd been told to build a life, and the life was the job. Now the password, which is the bit I think the whole case turns on. In New Jersey, in two thousand five, a search turned up a piece of paper reading alt, control, e, and then a string of twenty-seven characters. That string was the password to the program.



Corn

It was written down. On paper, in a house with a computer in it. It's always the paper.



Herman

It's almost always the paper. And the paper was only part of it. The FBI had also wired a townhouse in Boston, and in October two thousand four, one of the people in it, Tracey Foley, was recorded asking: Can we attach two files containing messages or not? Let's say four pictures...



Corn

So the pictures were never the secret. The microphone was.



Herman

The microphone heard them planning the pictures. That's the sentence that matters, more than any of the images.



Corn

So the most secure channel in the whole story was a conversation in a house with a microphone in it.



Herman

Number three, the porn video. In twenty eleven, an Austrian man named Maqsood Lodin, twenty-two years old, was questioned after coming back from Pakistan through Budapest. Investigators found a memory card, and a storage device, hidden in his underpants. The video on the card was called Kick Ass, and the file that mattered was marked Sexy Tanja. It took investigators weeks to crack the password and the software that went with it. What came out was more than a hundred documents. Manuals in German, English and Arabic. Reflections on past operations. And a document reported as Future Works, which brainstormed targets and methods, including a cruise ship hijack and Mumbai-style attacks.



Corn

So the one documented case of al-Qaeda, pornography and hiding is a file marked Sexy Tanja, in a video called Kick Ass, on a card in a man's pants. Of course it was in his pants.



Herman

Where else would you put it? Die Zeit's Yassin Musharbash broke the story, and CNN picked it up in May two thousand twelve. But I haven't seen the documents' wording quoted anywhere I can check, so I'm not going to read you any of it. We have the titles and the subjects. We don't have the sentences.



Corn

Who even opens a video like that looking for manuals?



Herman

Nobody does, and that's the design. Corn, if you were planning something, would you keep your manuals in a video?



Corn

The bet is that nobody checks the video. It's a good bet, too, right up until somebody's questioned at a border.



Herman

Number two. The most recent case, and the one with the strangest cover.



Corn

Go on.



Herman

June twenty seventeen, a security firm called ESET published research on a Russian group called Turla. The group had built a backdoor into a Firefox extension, and the extension took its instructions from comments on Instagram. One comment, posted under a photo of Britney Spears on the sixth of February, twenty seventeen, looks like this, to your eye: smith twenty-one fifty-five, hashtag two hot, make loveid to her, uupss, hashtag hot, hashtag X. And yes, loveid, spelled L O V E I D. That's how it's written.



Corn

Under a Britney Spears photo, a garbled, misspelled come-on with three hashtags is the least suspicious sentence you could ever write. It looks like every other comment there.



Herman

The message isn't in the words. Between the letters there are invisible characters, zero-width joiners, which display nothing at all, so to the reader the comment is just ordinary text. The extension reads the pattern those invisible characters make, pulls a hidden string out of them, and turns the string into a shortened web address. Before it acts on a comment, it works out a hash of that comment, and it only goes ahead if the result is one hundred and eighty-three.



Corn

So the comment is a dead drop, and the photo is the wrapper.



Herman

Why a comment at all? Because a comment is public, it sits there until someone deletes it, and the operator never has to talk to the target. The link pointed to a server that Turla had used before, in an earlier watering-hole campaign. ESET saw seventeen clicks on it in February, and their best guess was a test.



Corn

Seventeen clicks in a month. That isn't a campaign. That's a family.



Herman

Corn, would you have clicked?



Corn

I'd have clicked on the Britney photo, honestly.



Herman

Wrong click, Corn.



Corn

The hiding was clever, I'll give them that. And the people who caught it were taking apart a browser extension, which is the least glamorous job in the business.



Herman

That's always the job. The clever part gets the headline, and the taking apart gets the answer.



Corn

So the real question is where you'd put it.



Herman

Somewhere people look and don't read. That's the whole category, I think.



Hilbert

Corn, can you put a message in a photo of a piano, so only the one person who knows where to look gets it? I've been turning it over since the Britney bit. A man in Ashdod has eleven photos of a piano in the rain, and I think he's telling somebody something.



Corn

Eleven photos of a piano in the rain. Does it play?



Hilbert

Four hundred and twenty shekels, collect only. I rang him at twenty past eleven. He said the piano was in the flat of a dentist called Fima, on the third floor, over a shop that sells only doorbells. I went at two. The shop had forty-one doorbells in the window and not one of them worked.



Herman

Forty-one doorbells, none of them working. That's a shop with a theme.



Hilbert

Fima said the piano belongs to his tenant. Dov. Dov was a lift engineer for thirty-one years, and since he retired he plays the same four bars every evening at six, with the window open. Dov will sell the piano only to somebody who can play the four bars back to him. I played them. Dov said the third bar was flat. Dov was right.



Corn

So you were flat, and the lift engineer knew it before you did.



Hilbert

I had the four bars from a man called Gerald. I met Gerald once, on the ferry out of Piraeus. Gerald plays the piano. Gerald also ate twenty-six boiled eggs on the upper deck in forty-one minutes, and I have never once been allowed to forget that. He owes me eleven euros. He is the only man I know who has the four bars, so I rang him from the stairwell, and he played them down the phone, and he said I was a semitone out, which I was. So I went back up and played them again, and Dov came out on the balcony in a dressing gown and said, that's the one.



Herman

You rang a ferry man for a piano.



Hilbert

I rang him from the stairwell. Then I carried the piano down three flights with the doorbell man, who wanted to be paid in doorbells. I said no. He insisted. I had a piano like it once, and sold it to a man in Haifa, and he still hasn't paid the last of it. This one went in the back of a van, because I had the van for the afternoon.



Corn

You paid a doorbell man in doorbells.



Hilbert

Herman, you spent three minutes on the Pueblo before anybody asked for it. I was waiting.



Herman

Nobody's ever stopped me, Hilbert, and I'd like the record to show it isn't for want of people trying.



Hilbert

The listing is the only thing a buyer ever looks at, and the photos are the only honest part. The piano was never in the rain. It was in a stairwell the whole time, and the photos put it on a balcony. Corn, the thing I came out to ask. Would the thing you described let you put a message in a photo of a piano, so that one person reads it and the man who posted the photo doesn't know? I'm not saying why.



Corn

In principle, a picture can carry more than anybody sees in it. The hard part was never the hiding, though. It was the cover, and a piano on a balcony in the rain is a very good cover.



Hilbert

Fair. The listing's still up. It's a different piano now, in a different garden, in the rain.



Corn

Last one, and it's the darkest.



Herman

Number one. The case I'd put at the end of any list, and the one with the best payoff. In twenty eleven, the FBI published a codebreaking case in its own series, Cryptanalysts: Breaking Codes to Stop Crime. The letter at the center of it opens with an ordinary family greeting: Saludos loved one so today I heard from Uncle Moe over the phone.



Corn

That's a family letter.



Herman

It's about rehab, child custody and clean living. Then the cryptanalysts read every fifth word, and it says this: Today Moe told me he tested positive for methamphetamines the ninth of September but denies using and denies getting tested on ninth tested on the first. I'm waiting on paperwork. Got no witness of his recent usage. I feel if guilty of writeup he should be hit.



Corn

Every fifth word. Nobody counts the fifth word of a letter about child custody.



Herman

And there's no bounced envelope in this one, no caption, no scrap of paper. The cryptanalysts worked out the pattern, and then the FBI published it.



Corn

Clean living, rehab, custody, and then a hit order in the fifth word. You couldn't make that up if you tried.



Herman

Most people think the hard part of steganography is hiding the message.



Corn

The hard part is the cover. Every time, the cover was the boring bit, and the thing that gave the message away was something else entirely.



Herman

Next time somebody tells you the messages are hidden in the pictures, ask what the pictures are supposed to be. The boring answer is usually the right one.



Corn

Thanks to our producer, Hilbert Flumingtop, for holding the desk for this one.



Herman

This has been My Weird Prompts. If you liked it, leave us a review, or go to my weird prompts dot com.



Corn

We'll be back soon.