

The Call Is Coming From Inside the House

Challenging Attribution in Digital Evidence

The Next Fifty Minutes

THE CASE

Somebody hands you four records

Four records. All genuine. All pointing at one man.

THE ATTACK

How I built it

The same case, from the side of the person who did it.

THE QUESTIONS

What I'd want you to ask me

What these records actually support, and what to ask a technical person.

The goal: know what a record actually proves before you decide who did it.



professionally evil®

Kathy Collins

Senior Security Consultant | QSA

I break into things for a living

- **Penetration testing:** web applications, APIs, networks, and physical security
- PCI DSS Qualified Security Assessor

Which means I build the fakes.







About Secure Ideas

Founded in September 2010

- Kevin Tackett, CEO, former SANS instructor and author

Based in Jacksonville, FL

- Consultants work full-time as salaried employees and are located throughout the United States and Canada

Expert Security Consultants

- Penetration Testing and Vulnerability Assessments
- PCI Qualified Security Assessments (QSA)
- Security Architecture Reviews
- Education, including tabletops, training, and conference talks

Security Evangelists

- Teaching, Training, Sharing, Learning
- Avid open-source contributors
- Blog: blog.secureideas.com



Publicly recognized in Forbes, CNN, Fox News.
Performed expert Witness work for the FTC, DoJ, and various law offices and agencies

Copyright © 2026 Secure Ideas LLC

What is professionally evil®?

We are evil

- Our team needs to think **"evil"** so we can best understand how an attacker will behave, and what they will attack.

But we are also Professional:

- Our goal is to help companies improve their security posture.
- We have permission, Penetration Testing is *ALWAYS* conducted under contract.
- We establish and follow Rules of Engagement for every test.

Copyright © 2026 Secure Ideas LLC

The Case

THE LOSS

JaxSnax paid $340,000 to Crunch Supply Co.

Vendor of eleven years. Paid every quarter, to the same account, without incident.

This payment went to a different bank.

HOW IT SURFACED



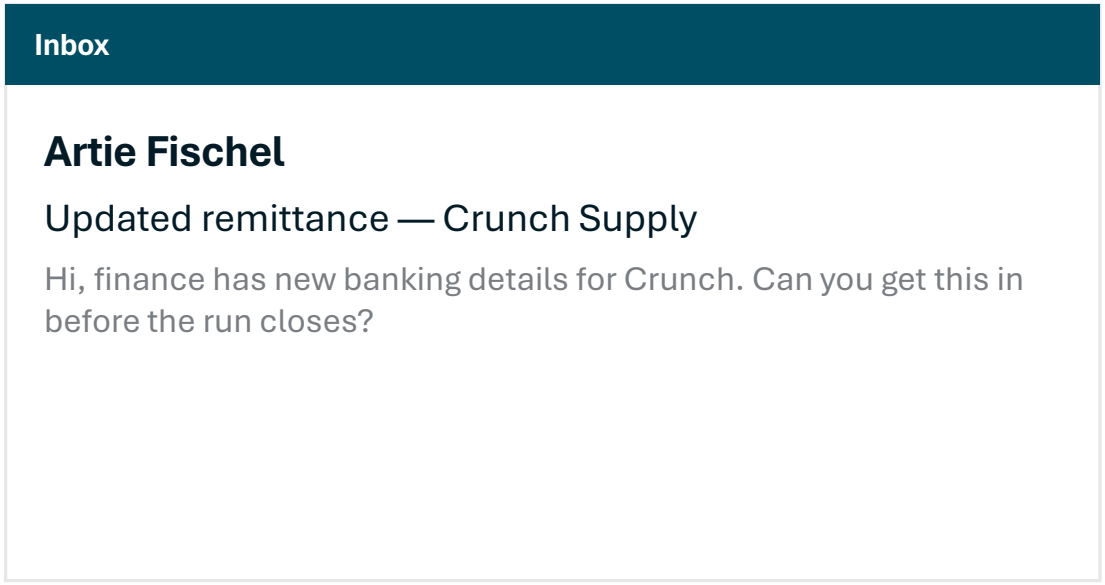
Day 6	**Crunch Supply calls**	“Where is our payment?”
Minutes later	**AP pulls the record**	The wire cleared. To an account nobody recognizes.
Same afternoon	**Recall attempted, and fails**	The funds moved within four hours of landing.

Find out how this happened, and who let it.

SecureIdeas professionally evil®

Exhibit A

AS IT APPEARED TO ACCOUNTS PAYABLE



Artie Fischel is the controller at JaxSnax. He has authorized vendor banking changes for nine years.

Exhibit B

JAXSNAX ERP AUDIT LOG

TIMESTAMP	USER	ACTION	RECORD
03/02 09:14	a.fischel	vendor.bank.update	CRUNCH-0041
03/02 09:18	a.fischel	payment.approve	WIRE-88213

The vendor record was changed and the payment approved four minutes apart.

Both actions under Artie's account. The log has no gaps and no errors.

Exhibit C

INBOX RULE FOUND IN ARTIE'S MAILBOX. CREATED 03/02, 08:51.

CONDITION	ACTION	ACTION
from contains “crunchsupply”	move to RSS Feeds	mark as read

THE WHOLE MORNING

08:51
Inbox rule created
Crunch Supply's emails hidden

← 23 minutes →

09:14
Vendor bank record changed
Where the money goes

← 4 min →

09:18
Payment approved
$340,000 released

Twenty-seven minutes, start to finish. The vendor was silenced before the money moved.

A rule that hides the victim's emails is not carelessness. It looks like a decision.

SecureIdeas professionally evil®

The Case Against Artie Fischel

- ✓ He asked for the banking change
- ✓ He made the change in the ERP
- ✓ He approved the payment four minutes later
- ✓ He hid the vendor's emails twenty-three minutes before that

Four records. All genuine.

And Four Audiences Are Waiting

HR	Insurer	The bank	Law enforcement
Termination decision	Crime or cyber claim	Recall and SAR	Possible referral

Four different standards of proof. One attribution underneath all of them.

If the name is wrong, it is wrong in four places at once, and the correction never travels as fast as the accusation.

Three Words That Get Collapsed Into One

Identification	Which account, device, or address was involved. The log gives you this for free.
Attribution	Which human was behind it. This is a hypothesis you add on top.
Proof	Whether that hypothesis survives counsel, an arbitrator, a regulator, or a jury.

Everything in Part One was identification. The case against Artie is attribution.

Before I Send Anything

Who matters	LinkedIn gives me the org chart. Controller, AP clerk, who reports to whom.
Who is away	Out-of-office replies tell me who is covering for whom, and when.
What you use	Job postings name your ERP, your email platform, your accounting stack.
Who you pay	Press releases, lawsuits, permits, and your own website name your vendors.
How you write	Breach data gives me your email format. First initial, last name, at your domain.

None of this touches your network. All of it is public.

This Part Is a Checklist

OSINT

- Public company data
- Employee data
- Domain and email discovery
- Breach data

PRETEXTS, PRE-WRITTEN

- Help desk: security update
- HR: direct deposit change
- Vendor: IT integration
- New meeting platform
- Exec assistant, on behalf of

WHAT MAKES THEM WORK

- Their industry's own terminology
- Keep it simple. Never over-explain
- Urgency, authority, or both

The same list runs against every company. Nothing on it was built for you.

The Domain

THEIRS

```
jaxsnax.com
```

MINE

```
jaxsnax-portal.co
```

Ten dollars. Four minutes.

Then I wait. A domain registered two days ago gets flagged by your mail filter. One registered six months ago does not.

Patience is the cheapest tool an attacker has.

One of These Is Real

`jaxsnax.com`	**Real**
`jaxsnacks.com`	**Spelled it out**
`jaxsnax-portal.co`	**Looks like infrastructure**
`jaxsnax.co`	**Dropped the m**

You are not going to catch this at 2:40 on a Friday.

What These Three Letters Actually Mean

SPF

Sender Policy Framework

A public list of which mail servers are allowed to send for a domain.

DKIM

DomainKeys Identified Mail

A cryptographic signature proving the message really came from that domain and was not altered.

DMARC

Domain-based Message Authentication

A published policy telling receiving servers what to do when the first two fail.

All three answer the same question: is this sender allowed to send for this domain?

And My Mail Passes All Three

SPF ✓	DKIM ✓	DMARC ✓

I set all three up on my domain. Correctly.

I own jaxsnax-portal.co. I publish its records. I sign its mail. So when a receiving server asks whether I am authorized to send for that domain, the honest answer is yes.

Passing authentication does not mean the domain is who you think it is.

It means the mail really is from wherever it says it is from.

Three Days Earlier

WHAT ARTIE GOT ON FEBRUARY 27

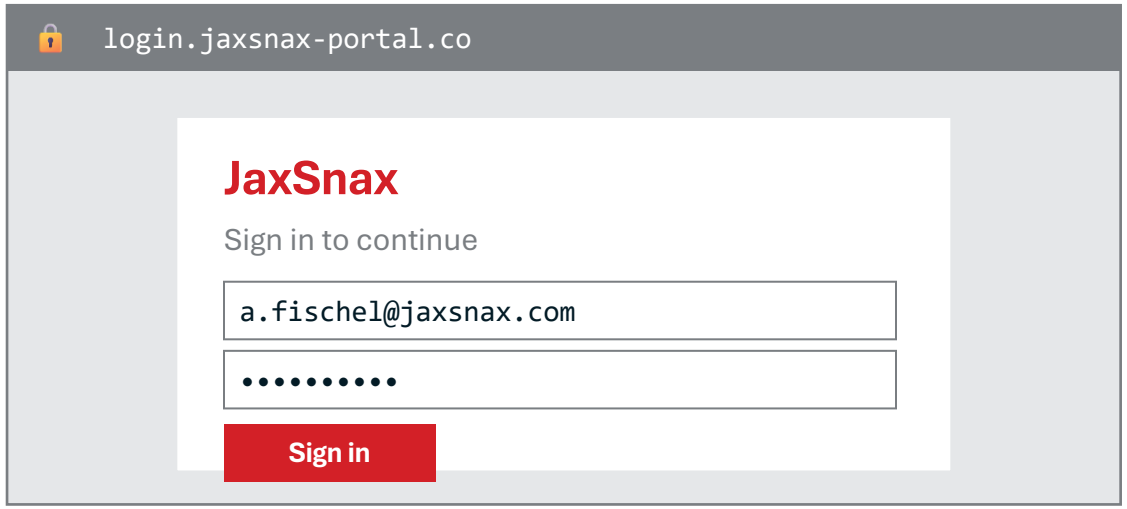
Inbox

JaxSnax IT

Action required: password expires today

Your JaxSnax password expires at 5:00 PM. Sign in to confirm your account and avoid interruption.

WHERE THE LINK WENT



THE TWO DATES

Feb 27 — **Artie gets an email. Looks normal to him. Nothing appears to happen.**

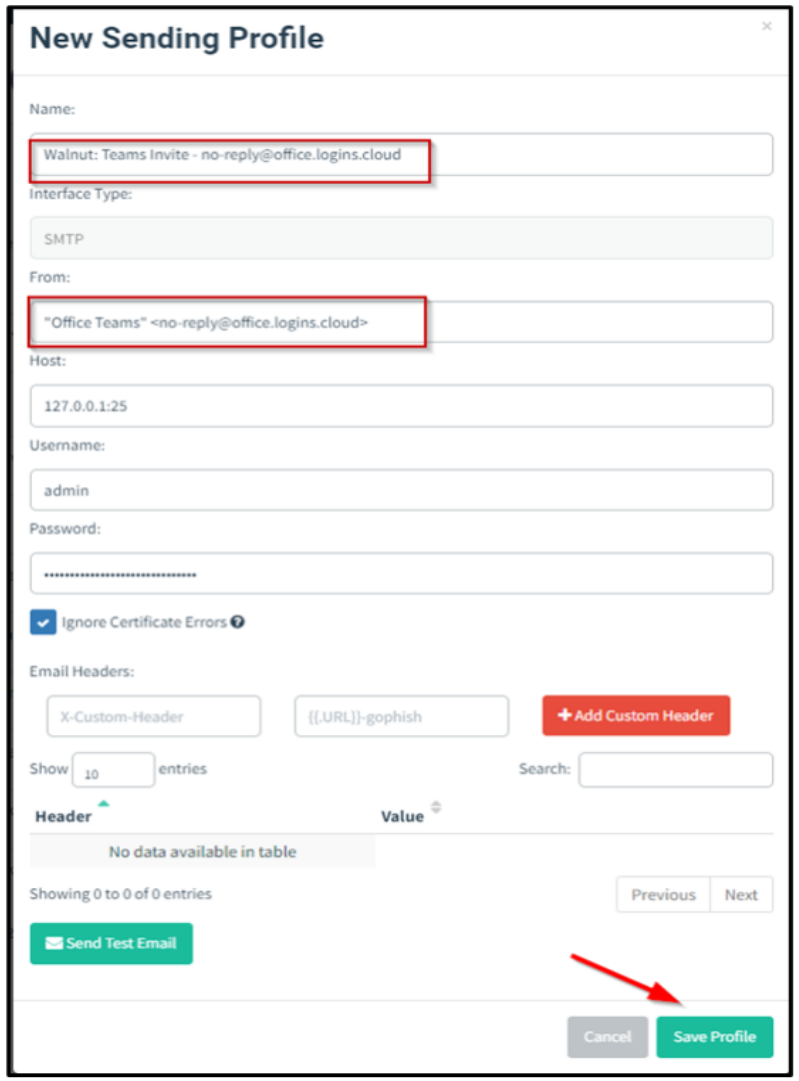
Mar 02 — **The wire goes out.**

Nobody pulled this email. It had nothing to do with a wire.

SecureIdeas professionally evil®

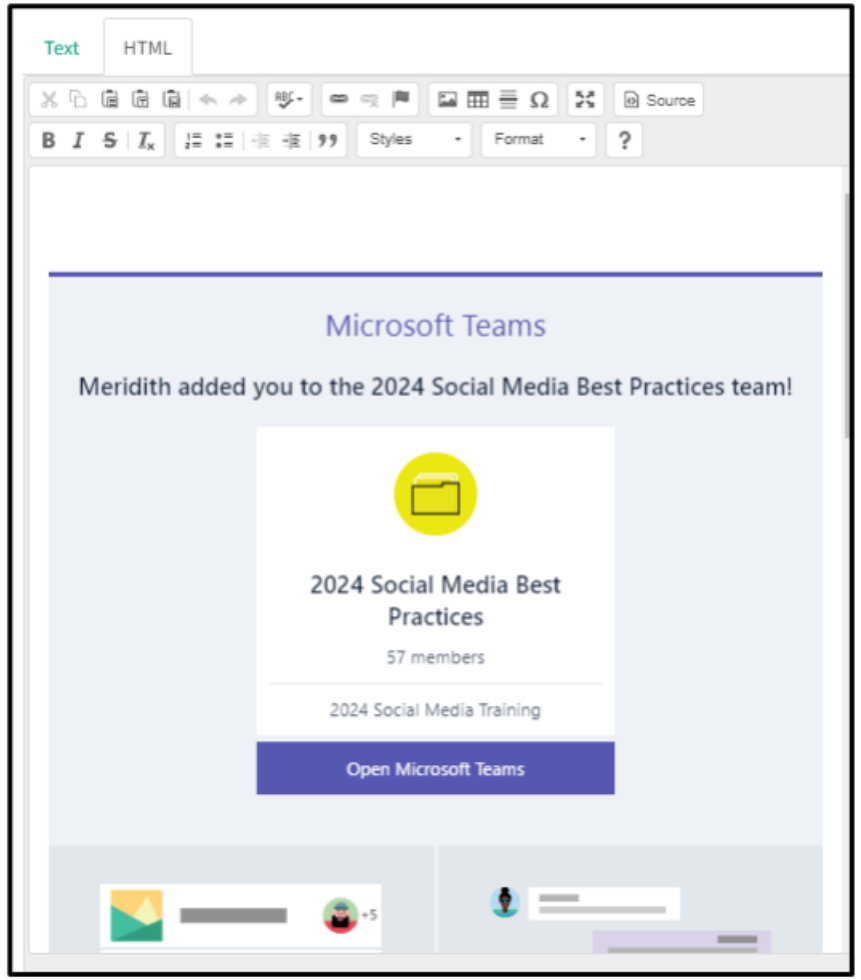
The Tooling Is Off the Shelf

SENDER CONFIGURATION





THE LURE, IN THE BUILDER

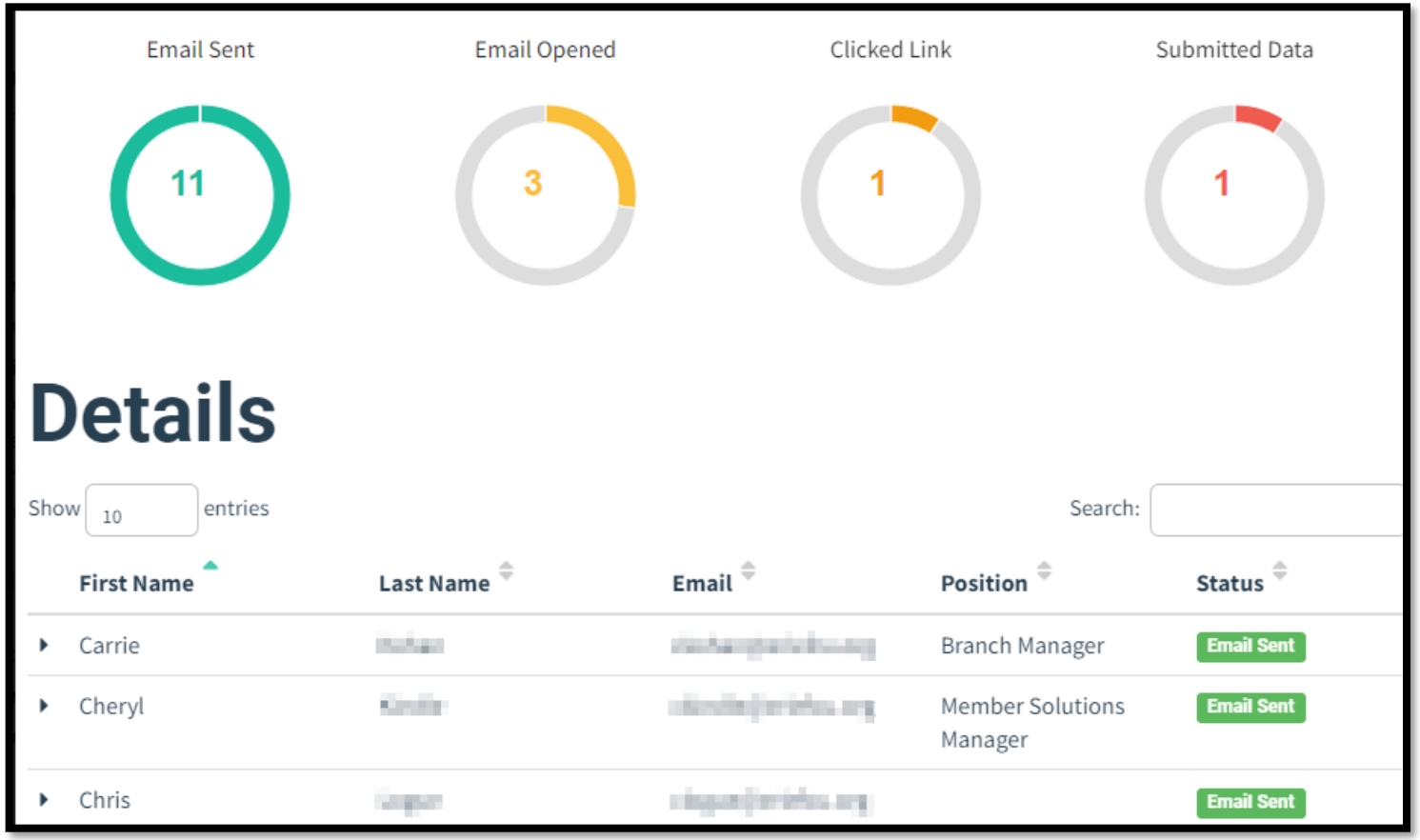


Name it, type the display name, build the email. That is the whole setup.

SecureIdeas professionally evil®

And Then You Just Wait

CAMPAIGN DASHBOARD



Eleven sent.

Three opened.

One clicked.

One submitted credentials.

One is all it takes.

SecureIdeas professionally evil®

One Password, Everything

Single sign-on

One login opens email, the software, the file shares, everything.

Artie's mailbox | **The ERP** | **Vendor records** | **Payment approval**

He typed it into my page once.

From that moment I am not pretending to be Artie Fischel. I am logged in as him.

First I Read

I did not send anything for three days.

The first thing you do in somebody else's mailbox is learn how they sound.

Sent items	Three hundred of Artie's emails. How he opens, how he signs, whether he uses contractions.
Threads	Who actually approves what, who pushes back, and who never does.
Attachments	A real JaxSnax remittance form, with your real formatting.

Minute Five: The Rule

EXHIBIT C. I CREATED THIS.

CONDITION	ACTION	ACTION
`from contains “crunchsupply”`	`move to RSS Feeds`	`mark as read`

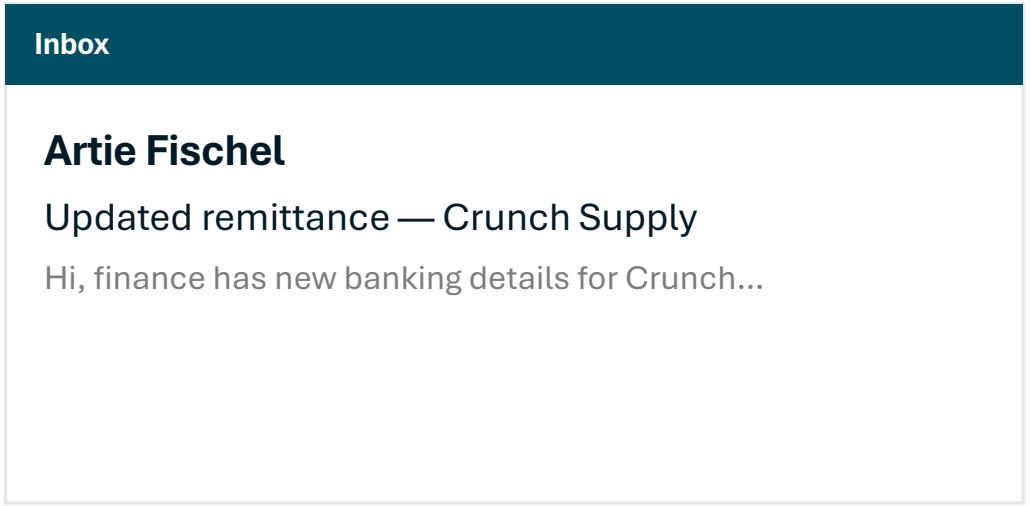
The first thing an intruder does in a mailbox is make sure the owner cannot see the conversation.

This was an incriminating artifact in the case. Concealment. A decision.

It was me. At 8:51. Before I touched anything else.

Then I Sent the Email

EXHIBIT A



AND THE HEADERS

From	a.fischel@jaxsnax.com
Domain	The real one.
Auth	SPF, DKIM, DMARC all pass.

This email was not spoofed. It came from Artie's actual account, on your actual domain.

There is no lookalike domain to find here. That trick was three days earlier, in a message nobody pulled.

And Then I Logged Into the ERP

EXHIBIT B, UNCHANGED

TIMESTAMP	USER	ACTION	RECORD
03/02 09:14	a.fischel	vendor.bank.update	CRUNCH-0041
03/02 09:18	a.fischel	payment.approve	WIRE-88213

I did not alter this log. I did not need to.

Same password, same single sign-on. The ERP let me in as the controller and recorded exactly what I did, under his name, because his account is what did it.

The log is not wrong. It answered a different question than the one you were asking.

Nothing in That Case Was Forged

The email	Real account. Real domain. Valid authentication.
The ERP log	Accurate. Complete. No gaps.
The inbox rule	Genuinely in his mailbox.
The timestamps	Correct to the second.

There was never anything to detect. Only something to ask.

And It Is Not Always an Attacker

Shared logins
One account, three shifts, no way to tell them apart

Service accounts
The actor is software, not a person

Delegated access
An assistant sending as the executive

Unlocked desks
Whoever is logged in, not whoever is sitting

Most broken attribution is not an attack at all.

It is an ordinary workplace arrangement that nobody thought of as an evidence problem until the day it became one.

Location and Time

GEOLOCATION LOOKUP

Address	198.51.100.42
Reported	Ashburn, Virginia
Reality	An estimate from a commercial database. Often the wrong city.

ONE EVENT, TWO CLOCKS

As logged	2026-03-14T02:17:44Z
As testified	March 13, 9:17 PM Eastern

A five hour offset can put an event on a day your suspect was demonstrably somewhere else.

SecureIdeas professionally evil®

When I'd Stand Behind a Record

One person, one credential	An account nobody else uses, shares, or administers
Multi-factor on that account	A second factor only that person holds
The system logs the actor	Not the mailbox owner, not the impersonated user
Independent corroboration	Badge data, a camera, a phone record, a second system
Behavior that fits	Or that does not, and the person can account for it

Attribution gets strong through convergence. One record alone never is.

Ask Your Technical Person These

- Who else can act as this account, and is that logged separately?
- Was multi-factor enabled, satisfied, and from what device?
- Which domain did that email authenticate for?
- When was that inbox rule created, and from what address?
- What did this account receive in the weeks before the incident?
- What time zone is this record in?

What I Could Actually Testify To

“These actions were taken using Artie Fischel's credentials.”	“Artie Fischel did this.”

I built every record in this case, and I can only support the one on the left.

The sentence on the right is not something the evidence says. It is something a person added.

What you do with that is your call. I just did not want you to make it without knowing.



Q & A

866.404.7837
secureideas.com

Copyright © 2026 Secure Ideas LLC

professionally evil®