
# The Hacker Did Not Destroy Your Evidence. Your Own Team Did.

*They probably acted in good faith.*

September 21, 2026 | 4-minute read | 920 words

▶ LISTEN · 8 MIN

DIGITAL FORENSICS

# The Hacker Did Not Destroy Your Evidence. Your Own Team Did.

*They probably acted in good faith. That is precisely why the case may no longer be defensible in court.*

## When Good Faith Weakens the Evidence.

Friday morning. A finance manager notices three wire transfers that do not belong. The CFO calls the IT department. IT does exactly what a competent technology team is trained to do: contain the problem and understand it quickly. During lunch, a support technician logs into the employee's computer with a shared administrator account, reviews the incoming and outgoing messages, copies the relevant folders onto a USB drive already used for other files, and restarts the computer, which had been behaving strangely.

That same afternoon, the employee resigns, effective immediately.

By Monday, management has a clear idea of what happened. It calls external counsel, who asks one question: who accessed that computer, when, and can you prove that nothing was altered afterward?

No one can answer. Four support technicians use the administrator account. The USB copy carries new timestamps rather than the originals. The restart cleared volatile memory and may have rotated logs that could have helped reconstruct the former employee's activity. The organization may understand the incident, but its ability to prove what happened has been seriously weakened.

Nothing was done in bad faith. Each action was intended to help. Yet each action altered or eliminated potential digital evidence and weakened the organization's ability to defend the case.





RISCCO

## What Digital Forensics Actually Is.

Technology teams are trained to restore operations and resolve incidents. A forensic examiner has a different responsibility: to preserve and reconstruct digital evidence so that it can withstand scrutiny in court.

Digital forensics determines what happened in a manner that holds up when someone with an incentive to discredit the conclusion examines every step. It requires acquiring data without modifying the source, using cryptographic verification to demonstrate the integrity of forensic copies, and documenting who handled the evidence, when, how and under whose authority.

Investigation asks what occurred. Forensics asks what you can still prove occurred six months later, before a judge or arbitral tribunal that did not witness the events.

## Reality. Not Science Fiction.

Many organizations associate digital forensics only with dramatic cyberattacks. The ordinary triggers are often less cinematic:

- An executive leaves for a competitor, taking confidential files containing the organization's expansion strategy.
- An employee alters the payroll payment file before submitting it to the bank for processing.
- An overseas supplier agrees by email to settle overdue payments owed to a local company. No contract addendum is signed, and the email correspondence—the only record of the agreement—is later deliberately deleted.

These situations share one condition: the digital evidence may eventually be tested in litigation, arbitration, an internal investigation or a regulatory proceeding. The standard is established when the evidence is first identified and collected. It cannot be applied retroactively.

In RISCCO's experience supporting legal counsel in digital evidence matters, some of the most damaging decisions occur before counsel or the forensic examiner receives the first call. Between the incident and the examiner's arrival, well-intentioned people may alter evidence while trying to understand or contain the problem.

## Technical Excellence Is Not Forensic Experience.

A strong systems auditor, cybersecurity specialist, database administrator or IT manager may be technically excellent. That does not automatically make the person a forensic examiner or an expert witness.

The difference is not only technical depth. It is the discipline to preserve evidence, demonstrate its integrity, distinguish facts from interpretation, document every relevant action and explain the conclusions to people without a technical background.

The written expert report is where otherwise sound technical work can fail. It must be precise enough to withstand scrutiny and clear enough that counsel, a prosecutor, a judge or an arbitrator can understand what happened, when it happened and how.

Then comes the part no certification alone can provide: defending the report while opposing counsel questions the methodology, tools, timing, chain of custody and even whether the examiner could have manipulated the evidence. The questions are stressful by design. Composure, clarity and professional judgment under that pressure are acquired through experience.

## Why RISCCO

RISCCO does more than determine what happened. We preserve what can still be proven.

For more than eight years, law firms and organizations have engaged RISCCO when a dispute, investigation or arbitration depends on understanding, preserving and defending digital evidence. We work alongside legal counsel from the first critical hours through forensic analysis, expert reporting and testimony.

Our digital forensics capability is supported by the same expertise RISCCO applies to IT risk, cybersecurity, data privacy, systems audit and data analytics. Our examiners therefore understand not only the device or forensic image, but also the control environment, systems and business processes surrounding the evidence.

- Dozens of digital forensic investigations and expert reports involving computer crime, fraud and security incidents, including matters before judicial authorities and international arbitral tribunals.

- Regular collaboration with external legal counsel, supported by a firm with 17 years of experience serving more than 200 organizations across Central America and the Caribbean.

In Panama, RISCCO conducts digital forensic investigations and provides qualified computer experts. In other jurisdictions, we can advise counsel and support locally qualified experts through forensic analysis, methodology, technical review and the preparation of findings, subject to local requirements.

If a digital incident may become a dispute, investigation or claim, preserve first and investigate second. Defensible digital evidence determines what you can prove.

*That is where RISCCO makes the difference.*

# CONTACT RISCCO

## Panama, Central America and the Caribbean

Antonio Ayala I.
CEO
aayala@riscco.com

Marinelda Morales
Sales Manager
mmorales@riscco.com

## Dominican Republic and Puerto Rico

Eury Valdez
Sales Advisor
efvaldez@riscco.com

## El Salvador, Guatemala, Honduras, Costa Rica and Nicaragua

Jeniffer Escoto
Sales Advisor
jescoto@riscco.com

**About RISCCO**

RISCCO is an independent international consulting firm committed to transforming how organizations manage risk and adopt Artificial Intelligence. We combine a rigorous GRC (Governance, Risk and Compliance) approach with advanced data analytics and Artificial Intelligence to help our clients anticipate risk, strengthen governance, and solve complex challenges. Headquartered in Panama and present in six countries, in 2026 we mark 17 years serving more than 200 leading organizations across Central America and the Caribbean.

International rigor. Agile execution. Measurable impact.
*We think like strategists. We execute like specialists.*

riscco.com