

UNVERIFIED

THE ROGUE PROTOCOL RED FLAG BRIEFING

A READER CHALLENGE

Five documents. One incident.
Can you spot what does not belong?

FILE 017

NO ISSUING AUTHORITY · READER EXERCISE ONLY · NON-CANONICAL

THE INCIDENT

Most manufactured outcomes do not look manufactured. Every individual document can be perfectly reasonable. The question is what happens when you put them in the same folder.

SCENARIO

At 02:17 on a Monday morning, a fire damages the records and communications annex at Bay Nine Transfer Yard, a private freight facility handling government and commercial cargo. The event is contained before sunrise. No fatalities are reported. The initial cause is listed as an electrical failure in a backup power cabinet. The local incident file is closed three days later.

YOUR TASK

You have five documents that were never meant to be read together. None proves wrongdoing. For each one, decide whether it is ordinary, unusual, or something you would preserve before the file closes.

READER CHECK

Do not ask, 'What proves a conspiracy?' Ask, 'What would I want to compare before I accept the official explanation?'

START HERE

THE OFFICIAL VERSION

FACILITY	Bay Nine Transfer Yard
EVENT	Electrical fire, records and communications annex
FIRST ALARM	02:17
RESPONSE	Local fire department + contracted site response
INITIAL CAUSE	Battery-backup cabinet fault
INJURIES	None reported
FILE STATUS	Closed 72 hours after incident
SUPPORTING PHRASE	No evidence of deliberate ignition identified

Nothing on this page is impossible. Fast closures happen. Electrical faults happen. A clean incident summary is not evidence of anything except a clean incident summary.

READER CHECK

If this were the only page you saw, what would you need before accepting the cause as settled?

THE WINDOW NO ONE NOTICED

23:41	BACKUP POWER SYSTEM	MAINTENANCE MODE ENABLED
00:02	REMOTE DIAGNOSTICS	DISABLED · 24-HOUR WINDOW
02:16	CAMERA NETWORK	OFFLINE
02:17	FIRE ALARM	ANNEX ZONE
02:21	EXTERNAL ALERT	TRANSMITTED
02:44	REMOTE DIAGNOSTICS	RE-ENABLED · ADMIN CREDENTIAL

Maintenance mode can be legitimate. A camera network can fail during a fire. The interesting question is not whether either event can happen. It is who controlled the maintenance window, and why an administrative credential restored access after the incident had already begun.

READER CHECK

Which record would you preserve first: the local log, the remote server log, or the identity behind the admin credential?

THE BADGE

BAY NINE TRANSFER YARD

SITE ACCESS

ROLE	SITE COORDINATION
ACCESS	ALL AREAS · ESCORT NOT REQUIRED
VALID	3 DAYS BEFORE INCIDENT → 1 DAY AFTER

ISSUED BY: EASTBRIDGE ADMINISTRATIVE SERVICES

Third-party staff carry third-party credentials every day. The red flag is not the existence of the badge. It is the combination of broad access, narrow timing, and a role description that explains almost nothing.

READER CHECK

Would you investigate the person on the badge, the company that issued it, or every other site where the same issuer appears?

THE COMPANY

BEHIND THE COMPANY

TASK ORDER	Emergency records recovery and site-security support
ACTIVATED	08:31, six hours after the first alarm
PRIME VENDOR	North Coast Asset Management
ADMINISTRATIVE SUPPORT	Eastbridge Administrative Services
PRIME ADDRESS	Suite 410, Herndon, Virginia
ADMIN ADDRESS	Suite 410, Herndon, Virginia
AUTHORITY	Standing emergency-services contract, active 18 months

Shared addresses are common. Standing contracts are common. Emergency activation is exactly what standing contracts are for. None of those facts is suspicious by itself. The question is why the same administrative layer appears in access, response, records handling, and follow-on work.

READER CHECK

When the same administrative entity touches every stage of an incident, is it background infrastructure, or the thing that connects the stages?

THE CLEAN ENDING

EVIDENCE ITEM	Original camera-network storage array
ACTION	Forensic image created
RETENTION	30 days after file closure
DISPOSITION	Recycled through approved electronics vendor
INDEPENDENT REVIEW REQUEST	Received day 33
ORIGINAL MEDIA	No longer available

Nothing here requires a villain. Evidence is retained, copied, and lawfully destroyed every day. The file can become impossible to revisit even when every person involved follows the written rule.

THE QUESTION:

What disappears when procedure works exactly as designed?

READER CHECK

If you thought the incident deserved a second look, where would you put the surviving copy so it could not be quietly dispositioned with the rest?

THE PATTERN

No single document proves a plot. That is the point.

The useful red flags are procedural, not theatrical.

Access appeared through an administrative layer. The same layer touched the response contract. The records system entered an unusual maintenance window. The file closed quickly. The original media disappeared on a lawful schedule before anyone asked to reopen it.

Any one of those facts can be ordinary. Put them together and you have a reason to preserve the originals, compare timestamps, and ask who benefits from every department doing its job exactly as written.

That is the recurring idea behind the Rogue Protocol universe: the most effective machinery does not require everyone to be corrupt. It only requires that no one person sees the whole sequence.

YOUR NEXT FILE IS NOT A TEST.

It is the Reader Vault.

READER ACCESS

OPEN THE READER VAULT

Free for J.D. Rourke readers. Delivered one classified file at a time.

PROTOCOL ZERO — the Rogue Protocol origin novella

THE CLEARPATH FILE — collected documents, Volume One

THE ROURKE FIELD GUIDE — survival principles behind the settings

UNLOCK ALL THREE

edenrootpress.com/j-d-rourke-reader-vault/

Scan the code or use the link. New files go to readers on the list first.

