

AN INVESTIGATIVE METHOD

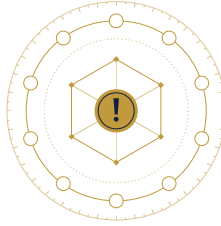


THE
WTF
METHOD

From Anomaly to Verified Intelligence

WTF → 5W+1H → THE LANDRY SCIENTIFIC INVESTIGATIVE LOOP

MARIE-SOLEIL SESHAT LANDRY



THE WTF METHOD

From Anomaly to Verified Intelligence

WTF → 5W+1H → THE LANDRY SCIENTIFIC INVESTIGATIVE LOOP

MARIE-SOLEIL SESHAT LANDRY

LANDRY INDUSTRIES INC. · MONCTON, NEW BRUNSWICK

THE WTF METHOD

From Anomaly to Verified Intelligence

First edition, October 2026

© 2026 Marie-Soleil Seshat Landry. Published by Landry Industries Inc., Moncton, New Brunswick, Canada.

The Landry Scientific Investigative Loop is an open research-method framework released by the author under the Creative Commons Attribution 4.0 International licence (CC BY 4.0).

Author ORCID: 0009-0008-5027-3337

AI DISCLOSURE

The source concept note for this method was drafted with Gemini 3.6 Flash, as declared in the original document. This book edition was expanded, edited and typeset with Claude Opus 5.5 (Anthropic) under the direction of the author. Historical and bibliographic claims were checked against live sources on 12 October 2026; see Sources & Further Reading.

SEO KEYWORDS

WTF Method, 5W1H Framework, Landry Scientific Investigative Loop, OSINT Methodology, Intelligence Analysis, Investigative Epistemology

SCENARIO NOTICE

The worked example in Chapter Seven and the ten example cases in Appendices 1–10 are invented scenarios. Their organizations, people, places, accounts, dates and data are fictional and exist only to demonstrate the method.

Set in Cinzel, EB Garamond and Poppins. Composed in HTML and rendered to PDF with WeasyPrint.

*I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.*

RUDYARD KIPLING · *Just So Stories* · 1902

CONTENTS

Preface	9
The Method at a Glance	11
PART I • THE TRIGGER	
1 The WTF Moment	15
PART II • THE STRUCTURE	
2 5W+1H Deconstruction	21
PART III • THE ENGINE	
3 The Loop at a Glance	27
4 Frame: Steps One to Four	31
1 · <i>Observe Anomaly</i>	31
2 · <i>Define Intel Requirement</i>	32
3 · <i>Hypothesize</i>	32
4 · <i>Design Experiment</i>	33
5 Test: Steps Five to Seven	35
5 · <i>Collect Verbatim</i>	35
6 · <i>Analyze</i>	36
7 · <i>Decision Loop</i>	37
6 Prove: Steps Eight to Ten	39
8 · <i>Conclusion</i>	39
9 · <i>Replicate</i>	40
10 · <i>Report</i>	40
PART IV • IN PRACTICE	
7 A Worked Example	45
8 The Ten Rules	49
APPENDICES 1–10 • EXAMPLE CASES	
1 The Lookalike Domain	52
2 The 3 a.m. Login Storm	54
3 The Phantom Citation	56
4 The Misattributed Quote	58
5 The Forty-Percent Claim	60
6 The Tuesday Temperature Drop	62
7 The Identical Comments	64
8 The Vanishing Vessel	66

THE WTF METHOD

9	The Backdated Memo	68
10	The Shutdown Rumour	70
BACK MATTER		
A	Field Templates	73
B	Glossary	77
C	Sources & Further Reading	79
	About the Author	81

PREFACE

WHY NAME IT THAT

Every investigation begins as a reaction before it becomes a method. Something does not fit. A timestamp contradicts a story, an account appears where none should exist, a claim circulates with total confidence and no traceable source. The first response is not analytical. It is visceral, and most investigators can name it in three letters.

This book takes that reaction seriously. It does not treat the jolt of surprise as noise to be suppressed on the way to “real” analysis; it treats it as the first sensor reading in a disciplined process. The WTF Method is a formal path from that first moment of cognitive friction to a finding that is verified, replicable and fit to report.

The path has three phases. The **WTF Moment** isolates the anomaly. **5W+1H Deconstruction** turns the reaction into six bounded vectors of inquiry. The **Landry Scientific Investigative Loop** runs those vectors through a ten-step engine built to reject what cannot be proven and keep only what survives.

None of the ingredients are new on their own. Asking who, what, where, when, why and how is older than the printing press. Testing ideas by trying to disprove them is the backbone of modern science. Weighing competing explanations against evidence is standard intelligence tradecraft. What the method adds is a single, repeatable sequence that joins them, so that the same discipline applies whether the anomaly is a line in a server log, a photograph in a news feed or an assertion in a research paper.

WHO THIS BOOK IS FOR

It is written for open-source intelligence practitioners, analysts, journalists, researchers and students: anyone whose work begins with noticing that something is off and ends with a statement other people will rely on.

HOW TO USE IT

Read it once straight through. The chapters follow the method in order, and each phase only makes sense in light of the one before it. After that, keep it near your desk. Chapter Eight condenses the whole method into ten rules that fit on a single page. Appendices 1 to 10 run ten more cases through the full method, each from a different field and each tied to one of the ten rules, and Appendix A gathers the field templates for every phase.



Marie-Soleil Seshat Landry
Moncton, New Brunswick · October 2026

INTRODUCTION

THE METHOD AT A GLANCE

The conversion from raw trigger to structured inquiry, and from structured inquiry to rigorous scientific and OSINT execution, is what formalizes intelligence tradecraft. The WTF Method makes that conversion explicit. It takes the initial cognitive friction of an investigation and turns it into a loop that is actionable, repeatable and verifiable.



FIGURE 1 · THE THREE PHASES OF THE WTF METHOD

THREE PHASES, ONE DIRECTION

Each phase has one job and hands a defined product to the next. The *WTF Moment* produces a precisely named anomaly, anchored to raw artifacts and stated against an explicit baseline. *5W+1H Deconstruction* produces six bounded vectors of inquiry: what is known, what is unknown and what must be collected for each. The *Loop* produces a verified conclusion, a record of

every hypothesis that was rejected and why, and a report that someone else can replicate.

The direction is always from feeling to fact. The method does not suppress intuition; it routes it. Intuition is welcome at the start, where it detects the anomaly, and in Step 3, where it proposes hypotheses. It is not welcome in Steps 5 and 8, where only verbatim evidence and verified statements are allowed.

THREE PRINCIPLES

PRINCIPLE I · FRICTION IS DATA

The moment something feels wrong is a measurement, not a mood. Record it precisely before it fades or hardens into a theory.

PRINCIPLE II · STRUCTURE BEFORE SPECULATION

Bound the problem with six questions before attempting to explain it. A well-posed question is half the investigation.

PRINCIPLE III · ONLY WHAT SURVIVES DISPROOF IS REPORTED

Hypotheses are built to be broken. What remains after honest attempts to break it, and after independent replication, is what goes in the report. Everything else is labeled as open.

PART

I

THE TRIGGER

Where every investigation begins: the moment something does not fit.

1

THE WTF MOMENT

Identify the precise anomaly without jumping to prematurely formed conclusions.

OPERATIONAL DIRECTIVE · PHASE I

Every inquiry needs a starting impulse. In most methods that impulse is left unnamed, as if investigations began with a neatly written question. They rarely do. They begin with a jolt: a mismatch, a surprise, a sense that the picture in front of you is wrong. The WTF Method names that jolt honestly and makes it the formal first phase.

1.1 THE CATALYST

The function of the WTF Moment is simple: it is the *catalyst for inquiry*. Its mechanism is the detection of an anomaly that disrupts baseline assumptions. That anomaly can take several forms, and learning to recognize each one sharpens the sensor.

ANOMALY CLASS	WHAT IT LOOKS LIKE
DATA MISMATCH	Two records that should agree do not. A creation date falls after the first archived copy of the thing it created; a stated location conflicts with the metadata of the file that supposedly came from there.
UNEXPECTED FOOTPRINT	A digital trace appears where none should exist: an account, a domain, a reused identifier, a file in the wrong place.

ANOMALY CLASS	WHAT IT LOOKS LIKE
UNVERIFIED ASSERTION	A claim circulates with confidence but no traceable origin. It may be true. It has simply not yet earned the right to be treated as true.
PATTERN BREAK	A regular rhythm changes without explanation: posting cadence, traffic volume, writing style, a price, a schedule.

1.2 NO ANOMALY WITHOUT A BASELINE

An anomaly is only visible against an expectation. “This is strange” always carries an unspoken second half: *compared to what I expected*. The first discipline of the WTF Moment is to write that expectation down. If the baseline stays implicit, it cannot be examined, and an unexamined baseline is where many investigations go wrong. Sometimes the anomaly is real. Sometimes the expectation was simply mistaken.

A useful formulation has two parts, stated side by side: *I expected X, because of Y. I observed Z*. The gap between X and Z is the anomaly. The reason Y is the baseline, and it should be as checkable as the observation itself.

1.3 THE DISCIPLINE OF NOT CONCLUDING

The WTF Moment is emotionally charged, and the mind’s first move after surprise is to explain it. The operational directive forbids exactly that. At this phase the investigator names the anomaly, not its cause.

NAME THE ANOMALY, NOT THE ANSWER

Premature: “This account is a coordinated fake.”

Disciplined: “This account was created recently and posted at a rate far above the baseline for accounts of its age in this community. The raw post log is preserved.”

The first statement has already skipped to a conclusion and quietly chosen among explanations. The second describes a deviation and leaves every ex-

planation open, including the dull ones. Dull explanations matter: error, coincidence and misunderstanding account for a large share of anomalies, and the method is designed to give them a fair hearing in Step 3.

1.4 CAPTURING THE MOMENT

Surprise fades and memory edits. The WTF Moment therefore ends with a written record, made before any analysis begins. The *WTF Log* (Template A. 1) captures six fields:

1. **Timestamp** of the observation, in UTC.
2. **Observer** and the context in which the anomaly was noticed.
3. **Raw artifact**: the unedited source, and where a preserved copy now lives.
4. **Expected baseline**, with the reason for expecting it.
5. **Observed deviation**, described without interpretation.
6. **Confidence that the deviation is real**, which is not the same as confidence in any explanation for it.

OPERATIONAL DIRECTIVE

Identify the precise anomaly without jumping to prematurely formed conclusions.

PART

II

THE STRUCTURE

Six honest questions that turn a reaction into a requirement.

2

5W+1H DECONSTRUCTION

Translate the visceral reaction into six distinct vectors of inquiry, and bound the scope of the investigation.

PHASE 2 · STRUCTURING INTEL REQUIREMENTS

A named anomaly is still only a question mark. Phase 2 breaks it into parts. Each of the six classic questions becomes a *vector*: a direction of inquiry with its own evidence types, its own collection sources and its own characteristic mistakes. Together they bound the investigation, defining what is in scope and, just as importantly, what is not.

2.1 A VERY OLD TOOLKIT

The six questions have a long pedigree. The Greek rhetorician Hermagoras of Temnos divided any subject into seven “circumstances”: who, what, when, where, why, in what way and by what means. He may have borrowed the scheme from Aristotle. In 1902, Rudyard Kipling set them to verse in the poem that follows *The Elephant’s Child* in his *Just So Stories*. Today they remain the journalist’s basic checklist for describing an event, and modern researchers still use them: one proposal, for example, applies 5W1H-based expression to sharing information in digital forensic investigations, on the grounds that it improves clarity and correctness.

The WTF Method keeps the six questions but sharpens each into an instrument of tradecraft.

VECTOR	INVESTIGATIVE FOCUS	PURPOSE IN TRADECRAFT
WHO	Entities, handles, networks, actors or infrastructure owners.	Target profiling & footprinting.
WHAT	Specific event, payload, payload behavior or assertion.	Defining the substance of the anomaly.
WHERE	IP addresses, GEOINT coordinates, domains or physical sites.	Spatial and spatial-digital context.
WHEN	Timestamps, epoch markers, log dates or historical sequence.	Temporal analysis & timeline mapping.
WHY	Motivation, strategic intent or underlying system mechanics.	Hypothesis generation.
HOW	TTPs (tactics, techniques, procedures), vector or mechanism.	Technical replication & verification.

TABLE 2.1 · THE SIX VECTORS OF INQUIRY



FIGURE 2 · SIX VECTORS RADIATING FROM ONE ANOMALY

2.2 WORKING EACH VECTOR

WHO · TARGET PROFILING & FOOTPRINTING

Which identities appear in the raw artifact? Which identifiers persist across platforms: usernames, email patterns, keys, profile images? Who owns or operates the infrastructure involved? *Common trap*: treating a handle as a person. A handle is an identifier; linking it to a human being is a separate claim that needs its own evidence.

WHAT · DEFINING THE SUBSTANCE

What exactly happened, stated in one sentence without adjectives? What is the payload: a file, a message, a claim, a transaction? What does it do when it runs, spreads or is read? *Common trap*: describing the interpretation instead of the event. “A malicious file” is a conclusion; “an attached file that opens a network connection on launch” is an observation.

WHERE · SPATIAL AND SPATIAL-DIGITAL CONTEXT

Where was the anomaly observed, and where did it originate? These are often different. Which physical features, coordinates or network records fix it in place? *Common trap*: treating the location of a server as the location of its operator, or the place where content was found as the place where it was made.

WHEN · TEMPORAL ANALYSIS & TIMELINE MAPPING

Normalize every timestamp to a single reference, preferably UTC, and record the original time zone beside it. Separate *first seen* from *first existed*. Build the sequence before interpreting it. *Common trap*: confusing the time something was published with the time it was captured, created or modified.

WHY · HYPOTHESIS GENERATION

What would make this anomaly rational? Which mechanisms could produce it with no intent at all? *Why* is where hypotheses are born, and also where bias is born. Keep its answers plural at this stage. A single answer to *why* before Step 3 is a conclusion in disguise.

HOW · TECHNICAL REPLICATION & VERIFICATION

What sequence of steps would reproduce the artifact? Which tools or procedures leave which traces? *How* is the most testable vector, because a proposed mechanism can often be re-run. *Common trap*: assuming sophistication. The simplest mechanism that reproduces the evidence deserves to be tested first.

2.3 BOUNDING THE SCOPE: THE GAP MATRIX

The six vectors also mark the edges of the investigation. For each one, write down three things: what is already *known and verified*, what is *unknown*, and what *collection* would close the gap. This is the Gap Matrix (Template A.2). It is the hand-off from Phase 2 to Phase 3. Every unknown becomes a candidate intelligence requirement in Step 2 of the Loop, and anything that fits none of the six rows is, by definition, out of scope for now.

VECTOR	KNOWN (VERIFIED)	UNKNOWN	COLLECTION NEED
WHO	Handle and creation date	Operator identity	Cross-platform identifier search
WHEN	Post timestamp (UTC)	Earliest appearance	Archive and reverse-search sweep
HOW	—	Production method	Metadata and artifact analysis

TABLE 2.2 · A PARTIAL GAP MATRIX (ILLUSTRATIVE)

PART

III

THE ENGINE

*The Landry Scientific Investigative Loop: ten steps from observation to a
report someone else can replicate.*

3

THE LOOP AT A GLANCE

The 5W+1H variables are fed directly into the ten-step execution engine to enforce zero-hallucination standards and rational rigor.

PHASE 3 · THE LANDRY SCIENTIFIC INVESTIGATIVE LOOP

The third phase is where the investigation is actually run. The Landry Scientific Investigative Loop takes the bounded vectors from Phase 2 and processes them through ten steps. It is called a loop rather than a list because one step, the Decision Loop, can send the work back to an earlier stage as many times as the evidence requires.

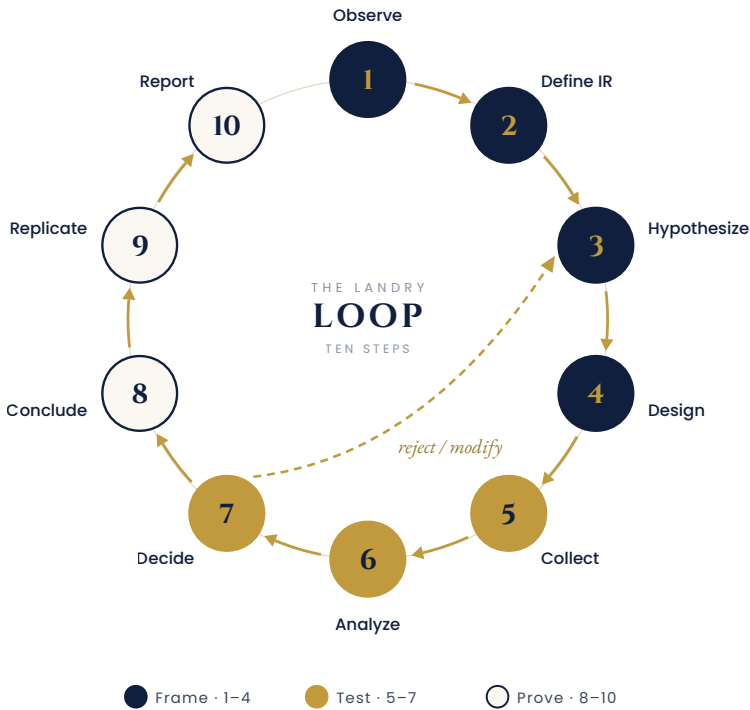


FIGURE 3 · THE TEN STEPS, GROUPED IN THREE ARCS, WITH THE REJECTION PATH FROM STEP 7 BACK TO STEP 3

3.1 THREE ARCS

The ten steps fall into three arcs, and the following three chapters take them in turn.

- **Frame (Steps 1–4).** Observe the anomaly, define the intelligence requirement, state falsifiable hypotheses and design tests meant to break them.
- **Test (Steps 5–7).** Collect verbatim facts, analyze them against every hypothesis, and reject or modify whatever the evidence contradicts.

- **Prove (Steps 8–10).** Record only verified conclusions, confirm that an independent run produces the same result, and deliver a standardized report.

3.2 BUILT TO DISPROVE

The Loop's core logic comes from the philosophy of science. In *Logik der Forschung* (1934; rewritten in English by the author as *The Logic of Scientific Discovery*, 1959), Karl Popper argued that no number of confirming experiments can prove a theory, while a single reproducible observation can refute one. A hypothesis that nothing could ever refute tells you nothing.

The Loop builds that asymmetry into its structure. Hypotheses must be falsifiable (Step 3). Tests are designed to disprove rather than confirm (Step 4). Contradicted hypotheses are rejected immediately (Step 7). Findings are not final until they reproduce (Step 9).

3.3 THE ZERO-HALLUCINATION STANDARD

The Loop is engineered against one failure in particular: stating something as fact that was never actually verified. It might come from a human analyst filling a gap with a plausible guess, or from an AI system producing fluent text with no source behind it. Either way, it is the same error. The defence is structural. Raw artifacts are preserved in Step 1, facts are collected verbatim in Step 5, and Step 8 admits only statements traceable to verified evidence. Each step narrows the space in which an unverified claim could slip through.

KINDRED FRAMEWORKS

The Loop sits alongside the author's other verification doctrines, notably Seshat's Axiom ($1 = 1 = 1$: *Retrieve = Store = Cite*) and the Landry Hallucination-Free Protocol. All share one premise: a claim is only as good as the artifact it can be traced back to.

4

FRAME: STEPS ONE TO FOUR

Before you collect anything, decide what would prove you wrong.

The first arc turns a named anomaly into a testable investigation. By the end of Step 4 the investigator has a preserved record of the anomaly, formal requirements, a set of hypotheses that can each be broken, and a plan for trying to break them.



STEP ONE · FRAME

OBSERVE ANOMALY

The WTF event

Document the exact deviation from baseline using unedited raw artifacts: raw logs, verbatim code, original OSINT captures. Step 1 formalizes the WTF Log from Phase 1 into an evidence record.

The governing rule is *preserve before you analyze*. Capture the artifact in its original form and record when, where and how it was captured. Where practical, compute a cryptographic hash (SHA-256, for example) so that anyone can later confirm the file has not changed. Analysis always works on copies; the preserved original stays untouched.

INPUT

WTF Log from Phase 1

OUTPUT

Anomaly Record with preserved, hashed raw artifacts

GUARDS AGAINST

Memory drift; “cleaned-up” evidence; lost sources

2

STEP TWO · FRAME

DEFINE INTEL REQUIREMENT

5W+1H mapping

Convert the deconstructed 5W+1H parameters into formal intelligence requirements (IRs) and collection targets. Each unknown in the Gap Matrix becomes a candidate IR. A good IR is specific enough that you will know when it has been answered.

IR STATEMENT PATTERN

Determine [*what is to be established*] regarding [*who / what*] in [*where*] during [*when*], in order to [*the decision or report it supports*].

Each IR is then paired with collection targets: the specific registries, archives, logs, datasets or sites where an answer could exist. An IR with no plausible collection target is a sign that the question needs to be reframed.

INPUT	Gap Matrix from Phase 2
OUTPUT	IR Register with numbered requirements and collection targets
GUARDS AGAINST	Scope creep; collecting everything and answering nothing

3

STEP THREE · FRAME

HYPOTHESIZE

Variable isolation

Formulate testable hypotheses $H_1, H_2 \dots H_n$ that address the *Why* and the *How*, and make sure each one is falsifiable. This is where intuition is invited back in. Generate widely, then write each hypothesis precisely enough to fail.

Two habits make this step work. First, always include the mundane explanation: error, coincidence, misconfiguration, misunderstanding. Second, attach a *kill condition* to every hypothesis, a sentence that begins “This hypothesis is false if we observe...”. A hypothesis without a kill condition is not yet ready to test.

INPUT	IR Register; the Why and How vectors
OUTPUT	Hypothesis Register ($H_1 \dots H_n$, each with a kill condition)
GUARDS AGAINST	Single-story thinking; unfalsifiable claims



STEP FOUR · FRAME

DESIGN EXPERIMENT

Designed to disprove

Develop targeted collection scripts, GEOINT verification protocols or OSINT search trees designed specifically to attempt to *disprove* H_n . The emphasis matters. A collection plan built to confirm a favored hypothesis will usually succeed, and prove very little.

Before collecting anything, write down what each hypothesis predicts you will find. Then favor *diagnostic* tests: those whose results would differ depending on which hypothesis is true. Evidence that is consistent with every hypothesis may be interesting, but it cannot help you choose between them.

INPUT	Hypothesis Register with kill conditions
OUTPUT	Collection Plan with predicted results per hypothesis
GUARDS AGAINST	Confirmation bias; non-diagnostic collection

5

TEST: STEPS FIVE TO SEVEN

Rejection is progress. Every hypothesis that falls narrows the space in which the truth can hide.

The second arc is where hypotheses meet evidence. Collection is strictly verbatim, analysis is structured, and the Decision Loop gives the method its name: whatever the evidence contradicts is dropped or rebuilt, and the investigation goes around again.



STEP FIVE · TEST

COLLECT

Verbatim facts only

Execute collection across primary sources: peer-reviewed literature, primary registries and official logs. Extract immutable facts without interpretation. In the evidence log, quote rather than paraphrase, record exactly where each fact came from and when it was retrieved, and keep the investigator's notes in a separate column from the facts themselves.

Rank sources by proximity to the event. A primary record outranks a report about it, and a report outranks a repost of the report. Where only secondary sources exist, say so in the log.

LAWFUL, ETHICAL COLLECTION

Open-source intelligence works from publicly available information. A widely cited U.S. statutory definition, from the National Defense Authorization Act for Fiscal Year 2006, describes OSINT as intelligence produced from publicly available information that is collected, exploited and disseminated in a timely manner to an appropriate audience to address a specific intelligence requirement. Collection under this method stays within the law and the terms of the sources used, and respects the privacy of people who are not the subject of a legitimate requirement.

INPUT	Collection Plan
OUTPUT	Evidence Log ($E_1 \dots E_n$), verbatim and sourced
GUARDS AGAINST	Paraphrase drift; unattributed facts; interpretation passing as data



STEP SIX · TEST

ANALYZE

Structured analytic techniques

Evaluate the collected data against every hypothesis using structured analytic techniques. The reference technique is the *Analysis of Competing Hypotheses* (ACH), developed by Richards J. Heuer Jr. at the U.S. Central Intelligence Agency in the 1970s and set out in detail in his book *Psychology of Intelligence Analysis* (CIA Center for the Study of Intelligence, 1999).

ACH places hypotheses across the top of a matrix and evidence down the side. Each cell records whether that item of evidence is consistent, inconsistent or neutral with respect to that hypothesis. The decisive move is to focus on *inconsistency*: hypotheses are judged by how much credible evidence contradicts them, and the least consistent are eliminated. Considering every hypothesis at once, rather than one favorite at a time, is what reduces cognitive bias.

EVIDENCE	H ₁	H ₂	H ₃
E ₁	C	I	C
E ₂	C	C	I
E ₃	N	I	C
Inconsistencies	0	2	1

TABLE 5.1 · C CONSISTENT · I INCONSISTENT · N NEUTRAL

INPUT	Evidence Log; Hypothesis Register
OUTPUT	Completed ACH matrix with notes on diagnostic evidence
GUARDS AGAINST	Satisficing; anchoring on the first plausible story

7

STEP SEVEN · TEST

DECISION LOOP

The rejection engine

If empirical evidence contradicts H_n , reject or modify it immediately, and return to Step 3 if necessary. This is the step that makes the method a loop. A modified hypothesis is a new hypothesis: it gets a new kill condition and goes back through design, collection and analysis.

Every rejection is logged together with the evidence that caused it. The rejected-hypothesis log is not an embarrassment to hide; it is part of the proof. It shows the reader which alternatives were considered and why they failed.

Exit conditions. Leave the loop when one of two things is true: a single hypothesis survives with no unresolved inconsistent evidence, or every reasonable avenue of collection has been exhausted, in which case the requirement is reported honestly as *undetermined*.

INPUT	ACH matrix
OUTPUT	Surviving hypothesis (or “undetermined”) and a rejected-hypothesis log
GUARDS AGAINST	Sunk-cost loyalty to a favored theory

6

PROVE: STEPS EIGHT TO TEN

If it cannot be replicated, it is not finished.

The final arc turns a surviving hypothesis into a deliverable. It is deliberately conservative. Only verified statements go into the conclusion, the conclusion must reproduce, and the report must carry everything a reader needs to check it.



STEP EIGHT · PROVE

CONCLUSION

Verified only

Record only statements supported directly by verified evidence or immutable facts. In practice, every line of the conclusion carries the evidence identifiers that support it (E₂, E₅...). A line that cannot be tagged does not belong in the conclusion.

What cannot be verified is not discarded. It moves to a separate section headed *Open Questions*, stated as questions rather than half-claims. Readers deserve to know where the verified edge of the investigation lies.

INPUT

Surviving hypothesis; Evidence Log

OUTPUT

Evidence-tagged findings; list of open questions

GUARDS AGAINST

Overreach; hedged speculation presented as fact



STEP NINE · PROVE

REPLICATE*Same inputs, same findings*

Validate that independent investigators or automated scripts produce identical findings given the same inputs and parameters. Package the investigation so that replication is possible: the preserved artifacts and their hashes, the exact queries and search parameters, the dates of collection, tool names and versions, and the procedure followed.

Then hand the package to a second analyst, or re-run the scripted portions from scratch. A discrepancy is not a failure of replication; it is a finding, and it sends the work back to Step 5 or Step 6 until the difference is explained.

INPUT	Findings; full method record
OUTPUT	Replication package and replication result
GUARDS AGAINST	Hidden steps; one-off luck; analyst-specific error



STEP TEN · PROVE

REPORT*The standardized deliverable*

Deliver the standardized output, either an *OSINT Intelligence Report* or a *LaTeX Technical Document*, containing an AI Disclosure, SEO Keywords and complete source attribution. The mandatory declarations are not decoration. The AI Disclosure tells the reader which automated systems touched the work; the keywords make the report findable; and full attribution lets any reader walk back from a finding to its evidence.

#	REPORT SECTION
1	Document metadata & mandatory declarations · AI Disclosure, SEO Keywords
2	Bottom line · verified findings, each tagged to evidence
3	Intelligence requirements · the IRs and their status
4	Method · the anomaly, the 5W+1H map, the collection plan
5	Evidence log · verbatim, sourced, timestamped
6	Analysis · ACH matrix and rejected-hypothesis log
7	Open questions · what remains unverified
8	Replication package · inputs, parameters, result
9	Sources · complete attribution

TABLE 6.1 · STANDARD REPORT SKELETON (TEMPLATE A.6)

INPUT	Everything above
OUTPUT	OSINT Intelligence Report or LaTeX Technical Document
GUARDS AGAINST	Undisclosed automation; untraceable claims; unfindable work

PART

IV

IN PRACTICE

*One anomaly, run through the whole method, and the method itself
reduced to ten rules.*

7

A WORKED EXAMPLE

The Flood Photograph

ILLUSTRATIVE SCENARIO · ALL DETAILS INVENTED

A photograph spreads quickly one spring morning. It shows a main street under brown floodwater, captioned “*Main Street right now. Get out while you can.*” The town is the fictional Riverton. The post has thousands of shares within the hour, and an analyst is asked whether it is real.

7.1 PHASE 1 · THE WTF MOMENT

The analyst’s first reaction comes before any tool is opened: the trees lining the street are in full summer leaf. In Riverton this week, the trees are still bare. That is the anomaly, stated as a data mismatch: *I expected bare trees, because local trees have not leafed out this season. I observed full foliage.* The image and the post are captured, hashed and logged. No conclusion is drawn.

7.2 PHASE 2 · 5W+1H

VECTOR	KNOWN	UNKNOWN → COLLECTION NEED
WHO	Posting account and its handle	Original photographer → find earliest publisher
WHAT	Image of a flooded street with a present-tense caption	Whether the image is unaltered → artifact checks
WHERE	Claimed: Riverton Main Street	Actual location → landmark comparison
WHEN	Post time (UTC)	Earliest appearance; date of capture → archive sweep
WHY	—	Poster's intent (may remain open)
HOW	—	Recycled, relocated or fabricated → tests below

7.3 STEPS 2–4 · FRAME

Intelligence requirements. IR-1: Determine whether the image depicts Riverton Main Street. IR-2: Determine the earliest verifiable online appearance of the image. IR-3: Determine whether Main Street was flooded on the date claimed.

Hypotheses. H_1 : genuine, current, Riverton. H_2 : genuine Riverton image from an earlier event, recycled. H_3 : genuine flood image from a different place. H_4 : manipulated or synthetic image. Each has a kill condition. H_1 , for instance, is false if the image appeared online before today.

Experiment design. Reverse-image and archive searches for the earliest copy (diagnostic between H_1 and H_2/H_3); landmark comparison against street-level imagery (H_3); the municipal advisory record for today (H_1); artifact inspection (H_4 , with the caveat that such tools are rarely conclusive on their own).

7.4 STEPS 5–7 · TEST

Collection produces five items, each logged verbatim with source and retrieval time:

- E_1 · The earliest copy found was published three years earlier.
- E_2 · Storefront signage and a church spire match current street-level imagery of Riverton Main Street.
- E_3 · Today's municipal advisory reports no flooding on Main Street.
- E_4 · Full foliage is inconsistent with the current season.
- E_5 · Artifact inspection finds no sign of manipulation (inconclusive).

EVIDENCE	H ₁ CUR- RENT	H ₂ RE- CYCLED	H ₃ ELSE- WHERE	H ₄ FABRIC- ATED
E_1 earlier copy	I	C	C	N
E_2 landmarks match	C	C	I	N
E_3 no flood today	I	C	C	C
E_4 foliage	I	C	N	N
E_5 no artifacts	C	C	C	N
Inconsistencies	3	0	1	0

TABLE 7.1 · FIRST PASS THROUGH THE MATRIX

Decision Loop, first pass. H_1 is rejected on three independent inconsistencies. H_3 is rejected on E_2 . But H_4 also shows zero inconsistencies, because nothing collected so far bears on it. The matrix cannot choose between H_2 and H_4 , so the loop returns to Step 4 to design a test that can.

Second pass. The new test looks for the context of the earliest copy. It yields E_6 : the three-year-old original was published by a local news outlet alongside a named photographer's credit and a report of that year's flood. E_6 is consistent with H_2 and inconsistent with H_4 . H_4 is rejected. H_2 is the sole survivor.

7.5 STEPS 8–10 · PROVE

CONCLUSION · VERIFIED ONLY

1. The image was published online no later than three years before the post under review. $[E_1, E_6]$
2. The image depicts Riverton Main Street. $[E_2]$
3. The municipal advisory for the date of the post reports no flooding on Main Street. $[E_3]$

Open question: Why the account presented an old image as current. Intent was not established and is not asserted.

Note what the conclusion does *not* say. It does not call the poster a liar, because the evidence speaks to the image, not to the poster's state of mind. *Why* stays an open question. That restraint is the method working as designed.

For Step 9, a second analyst re-runs the archive search with the same image hash, query parameters and date range, and finds the same earliest copy. The report is then issued with its AI Disclosure, SEO Keywords, evidence log, both matrices, the rejected-hypothesis log and full source attribution.

Ten more cases, from server logs and ship tracking to document forensics and research citations, follow in Appendices 1 to 10.

8

THE TEN RULES

The whole method, on one page.

I NAME THE ANOMALY, NOT THE ANSWER.

Describe the deviation; leave every explanation open.

II STATE THE BASELINE.

No anomaly exists except against an expectation you can check.

III PRESERVE BEFORE YOU ANALYZE.

Raw, unedited, hashed, and then work only on copies.

IV SIX QUESTIONS, EVERY TIME.

Who, What, Where, When, Why, How bound the scope.

V EVERY HYPOTHESIS MUST BE ABLE TO DIE.

Write the kill condition before you collect.

VI DESIGN TESTS TO DISPROVE.

Favor evidence that discriminates between explanations.

VII VERBATIM BEATS PARAPHRASE.

Facts in the log, interpretation in the margin.

VIII REJECTION IS PROGRESS.

Log what failed and why; it is part of the proof.

IX IF IT CANNOT BE REPLICATED, IT IS NOT FINISHED.

Same inputs, same parameters, same findings.

X REPORT WHAT IS VERIFIED; LIST WHAT IS NOT.

Disclose the AI, tag the evidence, attribute every source.

APPENDICES

1–10

EXAMPLE CASES

Ten anomalies from ten different fields, each run through the whole method from the first jolt to a verified report.

THE LOOKALIKE DOMAIN

A member of Tidewater Credit Union, a small regional lender, forwards an email asking members to “re-verify” their accounts before Friday. The message looks right. The sending domain does not: it differs from the credit union’s own by a single character, with *n* standing in for *m*.

PHASE 1 · EXPECTED

Member emails come only from the credit union’s registered domain.

OBSERVED · THE WTF MOMENT

A member email arrived from a domain one character different, linking to a login-style page.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Display name copies the credit union	Who registered and operates the domain
WHAT	Email with a link to a login-style page	What the page presents (observe only)
WHERE	The lookalike domain	Hosting and mail records
WHEN	Email received timestamp (UTC)	Domain and certificate creation dates
WHY	—	Hypotheses only
HOW	One-character substitution	Delivery and hosting mechanism

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1** Determine whether the credit union or an authorized agent registered the lookalike domain.
- IR-2** Determine when the domain and any TLS certificate for it came into existence.
- IR-3** Determine what the linked page presents to a visitor, without submitting any data.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	A defensive registration made by the credit union itself.	the credit union confirms it holds no such registration.
H ₂	Infrastructure built to impersonate the credit union.	the page and mail serve no credential-collecting function.
H ₃	A parked typo-domain earning ad revenue, unrelated to the email.	the domain sends mail and hosts a login form.
H ₄	An unrelated organization with a similar name.	the page copies the credit union’s branding.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁** The credit union’s IT manager confirms in writing that it holds no registration for the lookalike and has no agent who would.

- E₂** Registration data (RDAP) shows the domain was created four days before the email; registrant details are redacted.
- E₃** Certificate Transparency logs, which publicly record TLS certificates, show one issued for the domain a day after registration.
- E₄** Message headers show the email was sent through the lookalike domain’s own mail server.
- E₅** A sandboxed visit, with nothing entered, shows a login form copying the credit union’s logo, colours and wording.

EVIDENCE	H ₁ defensive	H ₂ impersonation	H ₃ parked	H ₄ unrelated
E ₁	I	C	C	C
E ₂	N	C	N	N
E ₃	N	C	N	N
E ₄	N	C	I	N
E ₅	N	C	I	I
Inconsistent	1	0	2	1

Decision Loop. One pass. H₁ falls on E₁, H₃ on E₄ and E₅, H₄ on E₅. H₂ survives with no inconsistent evidence.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. The credit union did not register the lookalike domain and has no agent who would have. [E₁]
2. The domain was created four days before the email; a TLS certificate for it was issued one day after creation. [E₂, E₃]
3. The email was sent through the lookalike domain’s own mail server. [E₄]
4. The linked page presents a login form copying the credit union’s branding. [E₅]

Open question. Who registered and operates the domain. Whether any member submitted credentials.

Replication. A second analyst re-queried the registration data and the certificate logs a day later and obtained the same dates.

RULE X REPORT WHAT IS VERIFIED; LIST WHAT IS NOT.

The credit union can file a takedown request and warn members using four verified facts. None of them requires naming the person behind the domain, and the report does not try.

THE 3 A.M. LOGIN STORM

Pageturn Books, a two-person online bookshop, wakes to an alert: about 2,300 failed logins against its admin panel between 03:00 and 03:20 UTC.

Every attempt targets the same account name, *backup-svc*. The owner's first message reads, simply, "Are we being hacked?"

PHASE 1 · EXPECTED

A handful of failed staff logins per night.

OBSERVED · THE WTF MOMENT

About 2,300 failures in twenty minutes, all against one service account.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Target account: <i>backup-svc</i>	Source of the attempts
WHAT	Failed logins, one account, no successes yet seen	Full request pattern
WHERE	Source addresses in the log	Ownership of those addresses
WHEN	03:00–03:20 UTC	What else is scheduled at 03:00
WHY	—	Hypotheses only
HOW	Admin login endpoint	Client signature (user-agent)

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1 Determine the source addresses of the attempts and who controls them.
- IR-2 Determine which automated processes are scheduled at or near 03:00 UTC.
- IR-3 Determine whether any attempt succeeded.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	An external credential-stuffing attack.	the attempts come entirely from infrastructure the shop controls.
H ₂	An internal job using an out-of-date credential.	no scheduled job uses that account.
H ₃	A staff member's misconfigured password manager.	the source is not a staff device.
H ₄	A security scan by the hosting provider.	the source is not a provider address.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁ All 2,300 requests came from a single address inside the shop's own hosting network.
- E₂ The user-agent string matches the backup tool installed on the shop's server.
- E₃ The backup job is scheduled daily at 03:00 UTC and retries on failure.
- E₄ The *backup-svc* password was rotated the previous afternoon; the job's configuration file still holds the old one.

E₅ No attempt succeeded; the account shows no successful login since the rotation.

EVIDENCE	H ₁ attack	H ₂ stale job	H ₃ staff	H ₄ scan
E ₁	I	C	I	I
E ₂	I	C	I	I
E ₃	N	C	N	N
E ₄	N	C	N	N
E ₅	C	C	C	C
Inconsistent	2	0	2	2

Decision Loop. One pass. Three hypotheses fall on E₁ and E₂. E₅ is consistent with every hypothesis and therefore decides nothing; it is reassuring, not diagnostic.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. All failed attempts came from one address inside the shop’s own hosting network, carrying the backup tool’s user-agent. [E₁, E₂]
2. The backup job runs at 03:00 UTC with retries, and its configuration held the pre-rotation password. [E₃, E₄]
3. No attempt succeeded. [E₅]

Open question. None on the cause. Adding a retry limit to the job is a recommendation, and is reported as one, not as a finding.

Replication. In a test window, the owner ran the job manually with the old configuration and reproduced the failure pattern exactly; with the new password, it succeeded on the first attempt.

RULE I NAME THE ANOMALY, NOT THE ANSWER.

The frightening explanation arrived first and felt obvious. Naming only the deviation kept the mundane explanation in play, and the mundane explanation was the right one.

THE PHANTOM CITATION

A literature summary drafted with an AI assistant cites a 2021 paper by Moreau and Okafor on the thermal stability of bio-based vitrimer composites, complete with journal, volume, pages and a DOI. It supports a key sentence in the summary. The analyst does not recognize it.

PHASE 1 · EXPECTED

A cited paper resolves through its DOI and appears in the journal's table of contents.

OBSERVED · THE WTF MOMENT

The DOI resolves to an unrelated article on soil chemistry.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Two named authors	Whether they exist and what they published
WHAT	A citation and the figure it supports	Whether any real paper matches
WHERE	Journal, volume, issue, pages	The issue's table of contents
WHEN	Stated year: 2021	Publication records
WHY	—	Hypotheses only
HOW	Produced in an AI-assisted draft	Which step introduced it

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1 Determine whether a paper with this title exists in any indexed source.
- IR-2 Determine what the DOI actually resolves to.
- IR-3 Determine whether any real source supports the figure attributed to the citation.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	A real paper with a wrong DOI or details.	the title is absent from the journal's contents and indexes.
H ₂	A real work in an unindexed venue.	neither author's publication record includes it.
H ₃	A blend of elements from real works.	no real work shares its authors, topic or claim.
H ₄	Invented with no real basis at all.	any real work matching its elements is found.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁ The DOI resolves to an unrelated 2019 soil-chemistry article.
- E₂ The stated issue's table of contents lists no such title; the cited pages belong to a different article.

- E₃** Title searches in Crossref’s metadata search and two scholarly indexes return no match.
- E₄** One named author published a 2018 paper on vitrimer thermal stability in another journal. Neither author’s record lists the cited title, and they have never co-published.
- E₅** That 2018 paper reports a different figure from the one the summary attributes to the citation.

EVIDENCE	H ₁ bad metadata	H ₂ unindexed	H ₃ conflation	H ₄ fabricated
E ₁	C	C	C	C
E ₂	I	C	C	C
E ₃	I	C	C	C
E ₄	N	I	C	I
E ₅	N	N	C	N
Inconsistent	2	1	0	1

Decision Loop. One pass. H₁ falls on E₂ and E₃; H₂ and H₄ fall on E₄. E₁ is consistent with everything; a broken DOI alone proves nothing about the paper.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. The cited DOI resolves to an unrelated 2019 article. [E₁]
2. No article with the cited title appears in the stated issue, in Crossref or in two scholarly indexes. [E₂, E₃]
3. The nearest real work is a 2018 paper by one named author, in a different journal, reporting a different figure. [E₄, E₅]

Open question. Which step of the drafting process introduced the citation.

Replication. A second analyst repeated the three title searches and the DOI resolution with identical results. The citation was removed and replaced by the verified 2018 paper and its actual figure.

RULE VII VERBATIM BEATS PARAPHRASE.

A citation is a claim, and it is checked against the source itself, never against a summary of it. If it cannot be retrieved, it cannot be cited.

THE MISATTRIBUTED QUOTE

A graphic circulates widely: “*The sea forgives no one who stops paying attention,*” attributed to Josephine Marchand (1871–1938), a lighthouse keeper whose logbook was published after her death. It is being quoted in a safety campaign. No source is given.

PHASE 1 · EXPECTED

A quote attributed to a historical person appears in her writings or in contemporary records.

OBSERVED · THE WTF MOMENT

No source is cited, and the same line is attributed online to three different people.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Three candidate speakers	Earliest attribution to each
WHAT	Exact wording, plus variants	Variant history
WHERE	Social media graphic	Earliest printed or digitized appearance
WHEN	Marchand died in 1938	Date of the earliest appearance
WHY	—	Hypotheses only
HOW	Shared graphic	First pairing of the line with her name

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1 Determine the earliest verifiable appearance of the exact wording.
- IR-2 Determine whether the line appears in Marchand’s published logbook.
- IR-3 Determine when the line was first attributed to Marchand.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	A genuine Marchand quotation.	it is absent from her writings and contemporary records.
H ₂	A paraphrase of something she wrote.	the line has a lineage independent of her writing.
H ₃	Coined by someone else, later misattributed.	no earlier appearance under another name exists.
H ₄	A recent invention.	it appears before the internet era.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁ Full-text searches of the digitized logbook, including wording variants, find no such line.
- E₂ The logbook contains a related idea in different words: a keeper who looks away is a keeper who will grieve.

- E₃** The earliest digitized appearance of the exact wording is a 1962 sailing-magazine column, credited to “an old fisherman.”
- E₄** The earliest pairing with Marchand’s name is a 2014 social-media post.
- E₅** Attributions to the two other figures all appear after 2016.
- E₆** *Second pass*: appearances between 1962 and 2014 run through fishing publications, none of which mentions Marchand or her logbook.

EVIDENCE	H ₁ genuine	H ₂ paraphrase	H ₃ misattributed	H ₄ recent
E ₁	I	C	C	C
E ₂	C	C	N	N
E ₃	N	N	C	I
E ₄	N	N	C	C
E ₅	N	N	C	C
E ₆	N	I	C	N
Inconsistent	1	1	0	1

Decision Loop. First pass (E₁–E₅): H₁ falls on E₁, H₄ on E₃. H₂ and H₃ both survive, so the loop returns to Step 4 to design a test that separates them. The second pass traces the line’s lineage (E₆), and H₂ falls.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. The exact line does not appear in Marchand’s published logbook. [E₁]
2. Its earliest digitized appearance is a 1962 magazine column crediting an unnamed fisherman. [E₃]
3. It was first paired with Marchand’s name in 2014. [E₄]

Open question. Who actually coined the line. The 1962 credit is itself unverified, and the report says so.

Replication. A second analyst ran the same archive queries, with the same variant list and date limits, and found the same earliest appearances.

RULE VIII REJECTION IS PROGRESS.

The first pass left two survivors. Rather than pick the likelier one, the loop went around again with a test built to kill one of them. The rejection of H₂ is what makes the result defensible.

THE FORTY-PERCENT CLAIM

A preprint on hemp-fibre composites states that a fibre treatment “improved tensile strength by 40% (Ref. 12).” The figure is about to be repeated in a grant proposal. A quick look at Ref. 12’s abstract shows a different number.

PHASE 1 · EXPECTED	OBSERVED · THE WTF MOMENT
A figure attributed to a reference appears in that reference.	Ref. 12’s abstract and results report a 28% improvement.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Preprint authors; Ref. 12 authors	—
WHAT	40% claimed versus 28% reported	How 40% was derived
WHERE	Preprint p. 4; Ref. 12 Table 3	Ref. 12 supplementary data
WHEN	Preprint version 1	Any later versions
WHY	—	Hypotheses only
HOW	Unstated calculation	Which baseline gives 40%

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1 Determine whether 40% appears anywhere in Ref. 12, including its supplementary information.
- IR-2 Determine whether 40% can be computed from Ref. 12’s data, and against which baseline.
- IR-3 Determine whether later preprint versions changed the figure or its wording.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	A transcription error for 28%.	40% can be derived from Ref. 12’s data.
H ₂	Computed from Ref. 12’s data against a different baseline.	no baseline in Ref. 12 yields 40%.
H ₃	The figure belongs to a different reference.	no other reference reports 40%.
H ₄	Not supported by any cited data.	40% is derivable from cited data.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁ Ref. 12 reports a 28% improvement relative to an untreated-fibre composite (Table 3).
- E₂ Its supplementary data include a neat-resin control. Treated composite: 42.0 MPa; neat resin: 30.0 MPa. The analyst computes a 40.0% increase.
- E₃ The preprint’s methods do not state which baseline was used.

- E₄** None of the preprint’s other references reports a 40% tensile improvement for this material.
- E₅** Version 2 of the preprint revises the sentence to “40% relative to neat resin (calculated from Ref. 12, Table S2).”

EVIDENCE	H ₁ typo	H ₂ other baseline	H ₃ wrong ref	H ₄ unsupported
E ₁	C	C	C	C
E ₂	I	C	N	I
E ₃	N	C	N	C
E ₄	N	N	I	N
E ₅	I	C	I	I
Inconsistent	2	0	2	2

Decision Loop. One pass. H₁ and H₄ fall on E₂ and E₅; H₃ falls on E₄ and E₅. E₁ fits every hypothesis, which is why the abstract alone could never have settled it.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. Ref. 12 reports a 28% improvement relative to untreated-fibre composite. [E₁]
2. Ref. 12’s supplementary data yield a 40.0% improvement relative to neat resin. [E₂]
3. Version 1 of the preprint did not state its baseline; version 2 does. [E₃, E₅]

Open question. None on the figure. The grant proposal should quote the number with its baseline, or quote both.

Replication. The calculation was published as a three-line script. A second analyst ran it against the supplementary table and obtained 40.0% and 28.0%.

RULE IX IF IT CANNOT BE REPLICATED, IT IS NOT FINISHED.

A number you can recompute is worth more than a number you can quote. Once the calculation was scripted, the disagreement disappeared: both figures were right, against different baselines.

THE TUESDAY TEMPERATURE DROP

A small materials lab is running resin-curing trials, and cure results are inconsistent. The room’s temperature logger shows something odd: a dip of about 4 °C beginning at 02:00 every Tuesday and lasting about ninety minutes, six weeks in a row.

PHASE 1 · EXPECTED	OBSERVED · THE WTF MOMENT
The room holds 22 °C ± 0.5 °C overnight.	A recurring 4 °C dip, Tuesdays from 02:00, lasting about ninety minutes.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Lab staff, facilities, night cleaners	Who has access at 02:00
WHAT	4 °C dip, about ninety minutes	Whether the dip is physical or instrumental
WHERE	Logger near the door and supply vent	Conditions inside the curing chamber
WHEN	Tuesdays 02:00, six weeks	What is scheduled then
WHY	—	Hypotheses only
HOW	—	Physical mechanism

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1 Determine whether the dip is a real change in air temperature or an artifact of the logger.
- IR-2 Determine what building systems or activities are scheduled on Tuesdays around 02:00.
- IR-3 Determine whether the dip reaches the samples inside the curing chamber.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	An artifact of the logger itself.	an independent instrument records the same dip.
H ₂	A scheduled building-system cycle.	the building schedule shows nothing at that time.
H ₃	A door opened by the night cleaning crew.	access logs show no entry at that time.
H ₄	Outdoor cold transmitted indoors.	outdoor temperatures show no matching pattern.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁ A second, independently calibrated logger placed beside the first records the same dip the following Tuesday.

- E₂** The building automation schedule shows a weekly air-handler cycle, Tuesdays 02:00–03:30.
- E₃** Door access logs show no entries between 22:00 and 06:00 on any of the six Tuesdays.
- E₄** Outdoor temperatures on the six nights varied widely and show no consistent drop at 02:00.
- E₅** A logger inside the curing chamber records a dip of 0.3 °C at the same time.

EVIDENCE	H ₁ logger	H ₂ HVAC	H ₃ door	H ₄ weather
E ₁	I	C	C	C
E ₂	N	C	N	N
E ₃	N	N	I	N
E ₄	N	N	N	I
E ₅	I	C	C	C
Inconsistent	2	0	1	1

Decision Loop. One pass. H₁ falls on E₁ and E₅, H₃ on E₃, H₄ on E₄. H₂ survives.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. Two independent loggers record the weekly dip. [E₁]
2. The dip coincides with a scheduled air-handler cycle, Tuesdays 02:00–03:30. [E₂]
3. No door entries occurred on those nights. [E₃]
4. Inside the curing chamber, the dip is 0.3 °C. [E₅]

Open question. Whether a 0.3 °C chamber dip affects cure outcomes. That is a separate experiment with its own requirement.

Replication. Facilities moved the cycle to Wednesday for one week. The dip moved with it, and Tuesday’s record was flat.

RULE VI DESIGN TESTS TO DISPROVE.

The second logger was the cheapest and most diagnostic test available: one result removed the instrument from suspicion and turned an annoyance into a finding.

THE IDENTICAL COMMENTS

A town's online consultation on a proposed wind project receives 37 comments with word-for-word identical text within two hours. A councillor asks the clerk's office whether the consultation is being flooded by bots.

PHASE 1 · EXPECTED

Public comments vary in wording and arrive spread over days.

OBSERVED · THE WTF MOMENT

37 identical comments within two hours.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	37 commenting accounts	Account history visible on the portal
WHAT	One identical text	Any earlier public source of the text
WHERE	The town's consultation portal	Portal submission records
WHEN	A two-hour window	Events just before the window
WHY	—	Hypotheses only
HOW	Portal comment form	Submission sources and devices

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1** Determine whether the wording appears in any earlier public source.
- IR-2** Determine whether the submissions came from one source or many, using the portal's own records.
- IR-3** Determine whether the accounts show public activity histories that predate the consultation.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	An automated bot network.	the accounts have long, varied histories and submissions come from many sources.
H ₂	A public template campaign by a real group.	no public template exists.
H ₃	One person using many accounts.	submissions come from many distinct sources.
H ₄	A portal glitch duplicating one comment.	there are 37 distinct submission records.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁** A residents' association published the exact wording in its public newsletter the previous evening, inviting members to copy and submit it.
- E₂** Portal records show 37 distinct submissions from 31 distinct network addresses, on a mix of device types.

- E₃** Of the 37 accounts, 33 were created more than a year earlier and have commented on unrelated consultations.
- E₄** Four accounts were created that day.
- E₅** Submission times cluster in the hours after the newsletter was sent.

EVIDENCE	H ₁ bots	H ₂ template	H ₃ one person	H ₄ glitch
E ₁	N	C	N	N
E ₂	I	C	I	I
E ₃	I	C	N	N
E ₄	C	C	C	N
E ₅	N	C	N	N
Inconsistent	2	0	1	1

Decision Loop. One pass. H₁ falls on E₂ and E₃; H₃ and H₄ on E₂. H₂ survives. Coordination was real; it was simply public and authentic.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. The wording was published as a template in a residents' association newsletter the evening before. [E₁]
2. The comments came from 37 distinct submissions across 31 network addresses. [E₂]
3. 33 of the 37 accounts predate the consultation by more than a year. [E₃]

Open question. Whether any of the four new accounts is inauthentic. Not established, and not pursued without a legitimate requirement to do so.

Replication. A second clerk re-ran the portal query for the same window and obtained the same counts.

RULE V EVERY HYPOTHESIS MUST BE ABLE TO DIE.

“Bot network” had a clear kill condition, and the evidence met it. Coordinated is not the same as inauthentic. Collection stayed at the level of public posts and the portal’s own records; no resident was profiled.

THE VANISHING VESSEL

On a popular ship-tracking site, a bulk carrier, the *Corran Bay*, disappears for nine hours while transiting a busy strait. A widely shared post claims the ship “went dark” to meet another vessel. The post includes a screenshot of the gap.

PHASE 1 · EXPECTED

Continuous AIS position reports from a vessel in busy coastal waters.

OBSERVED · THE WTF MOMENT

A nine-hour gap in one tracking provider’s data.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Vessel name and identifiers	—
WHAT	A gap in AIS position reports	Whether the gap exists in other sources
WHERE	One segment of the strait	Receiver coverage for that segment
WHEN	A nine-hour window	Same window for nearby vessels
WHY	—	Hypotheses only
HOW	Ship → receiver → provider → screen	Which link in that chain failed

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1 Determine whether the gap appears in an independent AIS data source.
- IR-2 Determine whether other vessels in the same segment show gaps at the same time.
- IR-3 Determine whether imagery places a vessel on the expected route during the window.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	The transponder was deliberately switched off.	an independent source shows continuous transmissions.
H ₂	A reception gap in that provider’s network.	nearby vessels show continuous data in that provider.
H ₃	An equipment fault aboard.	another provider received continuous transmissions.
H ₄	A provider-wide processing outage.	the provider’s data elsewhere is uninterrupted.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁ A second, independent AIS provider shows a continuous track for the vessel throughout the window.
- E₂ In the first provider’s data, eleven other vessels in the same segment show gaps over the same hours.

- E₃** The first provider's data elsewhere in the world shows no interruption during the window.
- E₄** The first provider's published coverage notes list the shore receiver for that segment as offline that day.
- E₅** Satellite imagery from the window shows a vessel of matching length at the position the second provider's track predicts.

EVIDENCE	H ₁ switched off	H ₂ coverage	H ₃ fault	H ₄ outage
E ₁	I	C	I	C
E ₂	N	C	N	C
E ₃	N	C	N	I
E ₄	N	C	N	N
E ₅	C	C	C	C
Inconsistent	1	0	1	1

Decision Loop. One pass. H₁ and H₃ fall on E₁; H₄ on E₃. The imagery (E₅) is consistent with every hypothesis: it shows where the ship was, not why the data stopped.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. An independent AIS provider recorded a continuous track for the vessel throughout the window. [E₁]
2. In the first provider's data, eleven other vessels in the same segment show gaps over the same hours; its data elsewhere is uninterrupted. [E₂, E₃]
3. The first provider listed its receiver for that segment as offline that day. [E₄]

Open question. None on the gap. The claim of a rendezvous is not supported by anything collected.

Replication. A second analyst pulled both providers' records for the same vessel identifiers and window and obtained the same tracks.

RULE IV SIX QUESTIONS, EVERY TIME.

The How vector did the work. Asking how a position reaches a screen (ship, then a shore or satellite receiver, then a provider) showed that a gap on one screen is a gap in one chain, not proof of a ship's behaviour.

THE BACKDATED MEMO

In a contract dispute between two small firms, one side produces a PDF memo dated 14 March 2019 that sets out a discount agreement. The other side says the agreement never existed. Both parties agree to let an independent analyst examine the file and the producing firm's mail archive.

PHASE 1 · EXPECTED

A memo dated 2019 carries metadata consistent with 2019.

OBSERVED · THE WTF MOMENT

The PDF's document information records creation in February 2025.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Author field; both firms	Who handled the file, and when
WHAT	Memo text, especially the pricing clause	Earlier versions of the text
WHERE	Produced as an email attachment	The producing firm's archives
WHEN	Dated 2019; metadata says 2025	Dates of any earlier version
WHY	—	Hypotheses only
HOW	Producer field names a word-processor export	Born-digital or scanned

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1 Determine the PDF's creation and modification metadata and the software that produced it.
- IR-2 Determine whether a 2019 version exists in the producing firm's archive.
- IR-3 Determine whether any archived version matches the PDF's content.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	A genuine 2019 memo, re-exported unchanged in 2025.	an archived version differs from the PDF.
H ₂	Created in 2025 and backdated.	a 2019 version with the same title exists.
H ₃	A genuine 2019 memo, later altered and re-exported.	the archived version is identical to the PDF.
H ₄	A scan of a 2019 paper original.	the PDF is born-digital.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁ The PDF's document information gives creation and modification dates in February 2025; the Producer field names a word processor's export function.
- E₂ The PDF is born-digital: a native text layer with embedded fonts and no scanned page images.

- E₃** The producing firm's mail archive holds an email dated 14 March 2019 with a word-processor attachment of the same title.
- E₄** The 2019 attachment matches the PDF word for word except clause 4, where the PDF adds one sentence on volume discounts.
- E₅** The 2019 attachment's own metadata shows creation on 13 March 2019 and last modification on 14 March 2019.

EVIDENCE	H ₁ re-export	H ₂ fabricated	H ₃ altered	H ₄ scan
E ₁	C	C	C	I
E ₂	C	C	C	I
E ₃	C	I	C	N
E ₄	I	N	C	N
E ₅	C	I	C	N
Inconsistent	1	2	0	2

Decision Loop. One pass. H₄ falls on E₁ and E₂; H₂ on E₃ and E₅; H₁ on E₄. H₃ survives.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. The PDF was created in February 2025 by a word-processor export and is born-digital. [E₁, E₂]
2. A memo with the same title was emailed on 14 March 2019; its file was created on 13 March 2019. [E₃, E₅]
3. The 2019 version and the PDF are identical except for one added sentence in clause 4. [E₄]

Open question. Who added the sentence, and when. File metadata is evidence about a file, not about a person, and cannot answer this alone.

Replication. Both files were hashed before examination. A second examiner, working from the hashed copies, reproduced the metadata readings and the text comparison.

RULE III PRESERVE BEFORE YOU ANALYZE.

Hashing both files before anyone opened them meant neither party could later claim the evidence had changed in the analyst's hands. Preservation came first, and everything else rested on it.

THE SHUTDOWN RUMOUR

A post on a regional farm forum claims that Bayview Hemp Processing “is shutting down next month—sell your bales now.” It is reposted dozens of times, and local buyers begin offering lower prices. Growers ask whether it is true.

PHASE 1 · EXPECTED

The closure of a major processor would be announced by the company and reflected in public records.

OBSERVED · THE WTF MOMENT

A single anonymous forum post, widely reposted, with no source.

PHASE 2 · 5W+1H

VECTOR	KNOWN	COLLECTION NEED
WHO	Anonymous poster; the company	—
WHAT	A claimed permanent closure	Company statements
WHERE	Regional farm forum	Company channels; business registries
WHEN	“Next month”	Timing of the first post
WHY	—	Hypotheses only
HOW	Reposts	Any real event behind the claim

STEPS 2–4 · REQUIREMENTS & HYPOTHESES

- IR-1** Determine whether the company has made any public statement about its operations.
- IR-2** Determine the company’s current status in the business registry.
- IR-3** Determine whether a similarly named entity has a recorded closure.

H	HYPOTHESIS	FALSE IF WE OBSERVE THAT...
H ₁	The company really is closing.	it announces continued operations and is registered as active.
H ₂	A temporary shutdown misreported as permanent.	no temporary shutdown was announced.
H ₃	Confusion with a similarly named company.	no similarly named entity has closed.
H ₄	Invented with no basis in any real event.	the claim traces to a real announcement or record.

STEPS 5–7 · EVIDENCE & ANALYSIS

- E₁** The company’s website and newsletter announce a two-week maintenance shutdown next month, with intake resuming afterward.
- E₂** The provincial business registry lists the company as active, with this year’s annual return filed.

- E₃** A company with a similar name in another province, Bayview Hemp Products, is listed in its registry as dissolved last month.
- E₄** The company posted new job openings this week.
- E₅** The earliest forum post appeared the day after the maintenance newsletter was sent.

EVIDENCE	H ₁ closing	H ₂ maintenance	H ₃ name mix-up	H ₄ invented
E ₁	I	C	C	I
E ₂	I	C	C	N
E ₃	N	N	C	I
E ₄	I	C	C	N
E ₅	N	C	N	N
Inconsistent	3	0	0	2

Decision Loop. First pass: H₁ falls on three items, H₄ on two. H₂ and H₃ both survive, and they are not mutually exclusive. No collection available could separate them, so the loop exits on its second condition: the origin of the rumour is reported as *undetermined*.

STEPS 8–10 · CONCLUSION & REPLICATION

CONCLUSION · VERIFIED ONLY

1. The company has announced a two-week maintenance shutdown, not a closure. [E₁]
2. It is registered as active and is currently hiring. [E₂, E₄]
3. A similarly named company in another province was dissolved last month. [E₃]

Open question. Which of these two events, or both, gave rise to the post: undetermined. The poster’s intent is not established.

Replication. A second analyst re-checked both registries and the company’s channels the next day with the same results.

RULE II STATE THE BASELINE.

Stating the baseline made the post anomalous in the first place: real closures leave records. The same baseline made the answer quick. The records existed, and they said something different.

APPENDIX A

FIELD TEMPLATES

Print, copy, fill in. One set per investigation.

WTF LOG		A.1 · Phase 1 / Step 1
TIMESTAMP (UTC)		
OBSERVER & CONTEXT		
RAW ARTIFACT & LOCATION		
HASH (SHA-256)		
EXPECTED BASELINE & WHY		
OBSERVED DEVIATION		
CONFIDENCE IT IS REAL		

5W+1H GAP MATRIX				A.2 · Phase 2
VECTOR	KNOWN (VERIFIED)	UNKNOWN	COLLECTION NEED	
WHO				
WHAT				
WHERE				
WHEN				
WHY				
HOW				

IR REGISTER			A.3 · Step 2
IR	DETERMINE ... REGARDING ... IN ... DURING ... IN OR- DER TO ...	COLLECTION TARGETS	
IR-1			
IR-2			
IR-3			
IR-4			

HYPOTHESIS REGISTER				A.4 · Steps 3 & 7
H	HYPOTHESIS	KILL CONDITION: "FALSE IF WE OBSERVE..."		STATUS
H1				
H2				
H3				
H4				
H5				

ACH MATRIX							A.5 · Step 6
EVIDENCE (ID · SUMMARY · SOURCE)		H1	H2	H3	H4	H5	
INCONSISTENCIES							

REPORT SKELETON		A.6 · Step 10
AI DISCLOSURE		
SEO KEYWORDS		
BOTTOM LINE (TAGGED)		
IRS & STATUS		
METHOD SUMMARY		
REJECTED HYPOTHESES		
OPEN QUESTIONS		
REPLICATION RESULT		
SOURCES		

GLOSSARY

ACH · ANALYSIS OF COMPETING HYPOTHESES

A structured technique, developed by Richards J. Heuer Jr., that evaluates all hypotheses against all evidence in a matrix and eliminates those with the most inconsistent evidence.

ANOMALY

A deviation between an observation and an explicit, checkable baseline. The object of the WTF Moment.

BASELINE

The stated expectation against which an anomaly is measured, together with the reason for holding it.

COLLECTION TARGET

A specific source (registry, archive, log, dataset, site) where an answer to an intelligence requirement could exist.

DECISION LOOP

Step 7 of the Loop. The rejection engine that drops or modifies hypotheses contradicted by evidence and returns work to Step 3 when necessary.

DIAGNOSTIC EVIDENCE

Evidence whose presence or absence differs depending on which hypothesis is true, and which therefore helps choose between them.

FALSIFIABILITY

The property of a hypothesis that it could, in principle, be shown false by an observation. Central to the philosophy of science of Karl Popper.

GEOINT

Geospatial intelligence: information tied to physical location, such as coordinates, imagery and mapped features.

IR · INTELLIGENCE REQUIREMENT

A formally stated question the investigation must answer, specific enough that it is clear when it has been answered.

KILL CONDITION

The observation that would prove a given hypothesis false, written down before collection begins.

OSINT

Open-source intelligence: intelligence produced from publicly available information, collected and disseminated to address a specific requirement.

REPLICATION PACKAGE

The artifacts, hashes, queries, parameters, dates, tools and procedure needed for an independent party to reproduce a finding.

TTPs

Tactics, techniques and procedures: the characteristic methods by which an actor or mechanism operates. The substance of the *How* vector.

VERBATIM COLLECTION

Recording facts exactly as they appear in the source, with provenance, and keeping interpretation separate.

ZERO-HALLUCINATION STANDARD

The requirement that no statement in a conclusion or report is presented as fact unless it traces to verified evidence.

APPENDIX C

SOURCES & FURTHER READING

Every source below was retrieved and checked on 12 October 2026.

1. Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999. Chapter 8, “Analysis of Competing Hypotheses.”
cia.gov/resources/csi/static/Psychology-of-Intelligence-Analysis.pdf
2. “Analysis of competing hypotheses.” *Wikipedia*. Retrieved 12 October 2026.
en.wikipedia.org/wiki/Analysis_of_competing_hypotheses
3. Popper, Karl. *The Logic of Scientific Discovery*. London: Hutchinson, 1959. First published as *Logik der Forschung*, Vienna: Julius Springer, 1934 (imprint 1935).
en.wikipedia.org/wiki/The_Logic_of_Scientific_Discovery
4. Kipling, Rudyard. *Just So Stories for Little Children*. London: Macmillan, 1902. “The Elephant’s Child,” followed by the poem “I Keep Six Honest Serving-Men.”
gutenberg.org/ebooks/32488
5. “Hermagoras of Temnos.” *Wikipedia*. Retrieved 12 October 2026.
en.wikipedia.org/wiki/Hermagoras_of_Temnos
6. Han, Jaehyeok, Jieon Kim and Sangjin Lee. “5W1H-based Expression for the Effective Sharing of Information in Digital Forensic Investigations.” arXiv: 2010.15711.
arxiv.org/abs/2010.15711
7. “Open source intelligence.” *The IT Law Wiki*, citing the National Defense Authorization Act for Fiscal Year 2006. Retrieved 12 October 2026.
itlaw.fandom.com/wiki/Open_source_intelligence
8. Landry, Marie-Soleil Seshat. “The WTF method: WTF → 5W+1H → Landry Scientific Investigative Loop.” Source concept note, 12 October 2026.

ABOUT THE AUTHOR

MARIE-SOLEIL SESHAT LANDRY

Marie-Soleil Seshat Landry is the CEO and founder of Landry Industries Inc., an incubator based in Moncton, New Brunswick, working across OSINT intelligence services, materials science research, AI governance and sustainability ventures. She has practiced open-source investigation for more than ten years and identifies professionally as an OSINT investigator and spymaster, operating as Marie Landry's Spy Shop.

Bilingual in English and French and self-taught, she is a prolific self-publisher of open research frameworks, among them Seshat's Axiom, the Landry Hallucination-Free Protocol, the FC/NV (Fact-Constant / Narrative-Variable) architecture and the Scientific Investigative 10-Step Loop at the heart of this book. Her middle name, Seshat, is also the namesake of her Seshat's Axiom.

ORCID 0009-0008-5027-3337 · [MARIELANDRYSPYSHOP.COM](https://marielandryspyshop.com)

EVERY INVESTIGATION STARTS WITH A JOLT. THIS IS WHAT TO DO NEXT.

Something does not fit: a timestamp, an account, a claim no one can source. *The WTF Method* turns that first moment of friction into a disciplined, repeatable path to verified intelligence.

In three phases, the WTF Moment, 5W+1H Deconstruction and the ten-step Landry Scientific Investigative Loop, it shows how to name an anomaly without jumping to conclusions, bound it with six honest questions, build hypotheses designed to be broken, and report only what survives.

- ◆ The ten steps, each with inputs, outputs and the error it prevents
- ◆ Analysis of Competing Hypotheses, made practical
- ◆ A complete worked example, from jolt to report
- ◆ Ten more example cases, across ten different fields
- ◆ Six field templates, ready to print

