

NON-NORMATIVE

$T = \sigma_v \quad \det = -1 \quad (x, y) \to (-x, y)$

"This reflects the standard."

Informative / Advisory (NOTE)

DNS Tool

Philosophical Foundations for Security Analysis Communication

Carey James Balboa

Independent DNS Security Researcher

ORCID 0009-0000-5237-9065 **DOI** 10.5281/zenodo.19468134

PROJECT dnstool.it-help.tech **SOURCE** github.com/IT-Help-San-Diego/dns-tool-intel

VERSION 26.51.0 · **LICENSE** BUSL-1.1

Companion artifact to "Confidence-Scored Analysis of Domain Security Infrastructure"

Abstract

This document describes the philosophical and analytical foundations that inform the communication architecture of DNS Tool — an OSINT platform for domain security analysis. While the primary methodology document addresses protocol science (RFC compliance, confidence scoring, calibration), this companion artifact addresses a distinct question: *why is the analysis structured and communicated the way it is?*

DNS Tool's analytical framework reflects deliberate application of classical analytical structures — Socratic questioning, Aristotelian rhetorical categories, and structured narrative architecture — to the problem of presenting security intelligence in a form that enables human decision-making across multiple professional contexts.

This document identifies those structures, traces their academic lineage, provides verifiable citations across both philosophical and computer science literature, and establishes the boundaries between protocol science, human factors, and philosophy of analysis — three disciplines that inform the platform but must not be conflated.

This paper is a companion to the primary methodology document.
See: dnstool.it-help.tech/methodology

1. Scope and Disciplinary Boundaries

1.1 Three Lanes

DNS Tool's methodology operates across three distinct disciplines. Each lane has its own standards of evidence, its own peer-reviewed literature, and its own criteria for correctness. Conflation between lanes — treating a rhetorical insight as protocol evidence, or a human factors finding as an RFC requirement — would undermine the rigor of all three.

LANE	DOMAIN	STANDARDS OF EVIDENCE	DNS TOOL IMPLEMENTATION
PROTOCOL SCIENCE	RFC compliance, DNS resolution, cryptographic verification	RFC specifications, IETF standards, reproducible queries	Analyzer engines, resolver consensus, DNSSEC validation
HUMAN FACTORS	Cognitive load, visual perception, decision-making under uncertainty	Peer-reviewed psychology, vision science, HCI research	Scotopic interface design, executive brief structure, information hierarchy
PHILOSOPHY OF ANALYSIS	Analytical reasoning structures, epistemic integrity, communication ethics	Classical philosophy, rhetoric, peer-reviewed communication and IS research	Five Perspectives architecture, verification workflow, confidence taxonomy

1.2 Interaction Without Conflation

These lanes interact — a protocol finding (Lane 1) is communicated through a visual hierarchy informed by cognitive research (Lane 2) using a rhetorical structure grounded in analytical philosophy (Lane 3). The interaction is by design. The conflation would be claiming that Aristotelian rhetoric validates a DNS finding, or that scotopic vision research changes an RFC requirement. It does not. Each lane validates within its own domain.

---

2. Socratic Verification: Elenchus in the Analysis Workflow

2.1 The Claim

DNS Tool implements a Socratic-inspired verification workflow: core security findings are paired with falsifiable questions and commands the reader can execute independently to test them.

2.2 Structure of the Elenchus

The Socratic method (*elenchus*) is a form of cooperative argumentative dialogue in which claims are tested through structured questioning, with the goal of exposing contradictions and arriving at justified conclusions (Benson, 2011; Vlastos, 1983). The method does not assert truth — it tests claims by inviting refutation.

DNS Tool's verification workflow mirrors this structure:

1. **Initial claim**: The platform presents an analytical finding (e.g., "This domain's SPF record authorizes the entire internet to send mail as this domain")
2. **Structured question**: The "Big Questions" framework reframes the finding as a falsifiable question (e.g., "Can this domain be impersonated by email?")
3. **Verification command**: A concrete `dig`, `openssl`, or `curl` command is provided so the reader can independently test the claim
4. **Resolution**: The reader either confirms the finding or identifies a discrepancy — in either case, the epistemic process is transparent

This is not a claim that DNS Tool conducts live Socratic dialogue with the user. It is a claim that the *structure* of the verification workflow — assert, question, provide means of refutation, resolve — follows the elenctic pattern.

2.3 Academic Grounding

In philosophy:

- Vlastos, G. (1983). "The Socratic Elenchus." *Oxford Studies in Ancient Philosophy*, 1, 27–58.
- Benson, H. H. (2011). "Socratic Method." In *The Cambridge Companion to Socrates*. Cambridge University Press.

In computer science:

- Wilson, J. D. (1987). "A Socratic approach to helping novice programmers debug programs." *ACM SIGCSE Bulletin*, 19(1). DOI: 10.1145/31726.31755
- Chidambaram, S. et al. (2024). "Socratic Human Feedback (SoHF): Expert Steering Strategies for LLM Code Generation." *Findings of EMNLP 2024*. DOI: 10.18653/v1/2024.findings-emnlp.908
- Krishnamurthy, B. et al. (2011). "A Socratic method for validation of measurement-based networking research." *Computer Communications*, 34(1). DOI: 10.1016/j.comcom.2010.09.014

Bridging claim: While the CS literature primarily applies Socratic method to pedagogy and code generation feedback, DNS Tool extends the pattern to *analytical verification* — the reader is not a student being taught but an analyst being equipped to independently falsify the platform's claims. This application appears uncommon in the OSINT and security tooling space, though not unprecedented in the broader software verification literature.

---

3. Aristotelian Analytical Categories and the Five Perspectives

3.1 The Claim

DNS Tool's Five Perspectives architecture — Intelligence Officer, DNS Engineer, Hacker, Executive, IT Pro — maps to Aristotelian analytical categories drawn from *Rhetoric* (ethos, pathos, logos) and *Nicomachean Ethics* (phronesis, techne). This mapping is structural, not decorative: each perspective embodies a distinct mode of analytical reasoning that corresponds to a classical category.

3.2 The Mapping

PERSPECTIVE	ARISTOTELIAN CATEGORY	FUNCTION	WHAT IT ASKS
The Intelligence Officer	**Ethos** (credibility, trustworthiness)	Quantifies what you can trust — ICAE measures accuracy, ICuAE measures currency, Unified Confidence carries epistemic weight	"How confident should I be in this finding?"
The DNS Engineer	**Logos** (logical argument, evidence)	Grounds findings in RFC specifications — not vendor interpretation, not blog posts, but the standards that define protocol correctness	"What does the standard actually say?"
The Hacker	**Pathos** (urgency, consequence awareness)	Reframes the same data through an adversarial lens — reveals attack surfaces, exposure vectors, the *stakes* of misconfiguration	"What can an attacker do with this?"
The Executive	**Phronesis** (practical wisdom, judgment)	Distills findings into strategic decisions — posture, risk, what needs attention, what is secure	"What do I need to decide?"
The IT Pro	**Techne** (craft, applied skill)	Translates findings into actionable remediation — provider-aware steps, TTL tuning, concrete next actions	"What do I need to fix?"

3.3 Academic Grounding

In classical philosophy:

- Aristotle. *Rhetoric* (c. 350 BCE). Book I, Chapters 2–3 (ethos, pathos, logos).

• Aristotle. *Nicomachean Ethics*, Book VI (phronesis, techne).

In peer-reviewed communication science:

• Alderman, C. (2018). "Ethos, pathos, logos: a script for clinical communication." *Journal of Pharmacy Practice and Research*, 48(4). DOI: 10.1002/jppr.1468

In peer-reviewed information systems and cybersecurity:

• Rife, M. C. (2010). "Ethos, Pathos, Logos, Kairos: Using a Rhetorical Heuristic to Mediate Digital-Survey Recruitment Strategies." *IEEE Transactions on Professional Communication*, 53(4). DOI: 10.1109/TPC.2010.2052856
• Johnston, A. et al. (2023). "Seeking rhetorical validity in fear appeal research: An application of rhetorical theory." *Computers & Security*, 125. DOI: 10.1016/j.cose.2022.103020
• Johnston, A. C. & Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors." *MIS Quarterly*, 34(3). DOI: 10.2307/25750691

In phronesis and engineering judgment:

• Arrichiello, V. (2016). "Systems Engineer: the ultimate phronetic leader?" *INCOSE International Symposium*, 26(1). DOI: 10.1002/j.2334-5837.2016.00263.x
• Malik, A. et al. (2020). "Phronesis in Medical Ethics: Courage and Motivation to Keep on the Track of Rightness in Decision-Making." *Health Care Analysis*, 28. DOI: 10.1007/s10728-020-00398-7
• Hylving, L. & Koutsikouri, D. (2016). "Putting Phronesis to Work in Digital Innovation." *HICSS 2016*. DOI: 10.1109/HICSS.2016.574

3.4 Disciplinary Note

The Aristotelian mapping describes the *communication and analytical structure* of DNS Tool's output — not its protocol science. The RFC compliance of an SPF record is determined by RFC 7208, not by Aristotle. The *decision* to present that finding through five distinct analytical lenses, each optimized for a different mode of reasoning, is the philosophical design choice documented here.

---

4. Narrative Architecture Matrix

4.1 Purpose

The Narrative Architecture Matrix is an infrastructure artifact — not a style guide. It maps every content zone in the platform to its story structure, applicable narrative lenses, claim protection status, and the archetype(s) it primarily serves. The goal is maintainability: if a new analytical framework is incorporated in the future, the matrix shows exactly which content zones it touches and which claim boundaries it must respect.

4.2 Definitions

Story Structure: The narrative pattern governing how information is sequenced within a content zone.

Narrative Lens: An optional layer of voice, metaphor, or framing that can be applied across archetypes. Lenses are applied to creative-safe content only — never to protected claims.

Claim Protection Status:

- **PROTECTED**: Facts, citations, methodology statements, RFC references, mathematical claims, and verified philosophical citations. Immutable without verifiable evidence.
- **CREATIVE-SAFE**: Metaphor, voice, tone, introductory framing, contextual prose. May be revised for style, clarity, or philosophical alignment.

4.3 The Matrix

CONTENT ZONE	STORY STRUCTURE	PRIMARY ARCHETYPE(S)	CLAIM STATUS
Origin Story	Monomyth (Hero’s Journey — Campbell’s comparative narrative structure, not “myth” in the sense of something false)	All	CREATIVE-SAFE
Five Perspectives	Aristotelian Categories	All	PROTECTED (structure) / CREATIVE-SAFE (prose)

Verification Principle	Socratic Elenchus	Intelligence Officer, DNS Engineer	PROTECTED
Big Questions	Socratic Elenchus	Executive, IT Pro	PROTECTED (questions) / CREATIVE-SAFE (framing)
Protocol Findings	Kishōtenketsu	DNS Engineer, Intelligence Officer	PROTECTED
Executive Brief	Consequence Framing + Phronesis	Executive	PROTECTED (findings) / CREATIVE-SAFE (framing)
Priority Actions	Fichtean Curve	IT Pro, DNS Engineer	PROTECTED (fixes) / CREATIVE-SAFE (headers)
Drift Timeline	Rebirth / Rags-to-Riches	All	PROTECTED (data) / CREATIVE-SAFE (prose)
Covert Recon Mode	Adversarial Reframing	Hacker	PROTECTED (findings) / CREATIVE-SAFE (voice)
Confidence Docs	Logical Exposition	Intelligence Officer	PROTECTED
Methodology (primary)	Scientific Paper	DNS Engineer, Intelligence Officer	PROTECTED
This Document	Academic Companion	All	PROTECTED (citations) / CREATIVE-SAFE (prose)
EDE Register	Epistemic Disclosure	Intelligence Officer	PROTECTED
Badges	Visual Summary	All	PROTECTED (data) / CREATIVE-SAFE (layout)

MISSION.md	Manifesto / Declaration	All	PROTECTED (principles) / CREATIVE-SAFE (voice)

4.4 Narrative Lenses Registry

Lenses are NOT archetypes. They are voice/framing layers that can be applied to CREATIVE-SAFE content across any archetype.

LENS	DESCRIPTION	PRIMARY AFFINITY	APPLICATION BOUNDARY
Fable	Mythology, metaphor, wisdom stories, narrative patterns from classical tradition	The Hacker	Intros, outros, contextual framing. Never on findings, never on citations.
Logic Chain	Step-by-step reasoning, mathematical proof structure, RFC citation chains	The DNS Engineer	Findings, methodology, verification commands. Always PROTECTED.
Tactical	Mission-oriented, adversarial framing, time-to-fix urgency	The Hacker, The IT Pro	Covert mode, remediation, attack surface descriptions.
Consequence	Business impact, risk quantification with confidence qualifiers, strategic clarity	The Executive	Executive brief, posture summaries, Big Questions framing.
Practical	Step-by-step instructions, provider-aware guidance, copy-paste commands	The IT Pro	Remediation, TTL tuner, fix steps. Always PROTECTED for commands.
Epistemic	Confidence levels, uncertainty quantification, calibration transparency	The Intelligence Officer	Confidence documentation, ICAE/ICuAE, EDE register. Always PROTECTED.
Founder's Voice	Personal, direct, metacognitive — the voice of the builder reflecting on the process	All (contextual)	Mission statement, origin story, EDE philosophical context. CREATIVE-SAFE.

4.5 Future Extension Protocol

When a new philosophical, analytical, or scientific framework is proposed for incorporation:

1. **Identify the lane** (Protocol Science, Human Factors, or Philosophy of Analysis)

2. **Verify academic standing** with peer-reviewed citations in the relevant lane
3. **Map to the matrix** — which content zones does it touch?
4. **Respect claim boundaries** — does it affect PROTECTED or CREATIVE-SAFE content?
5. **Cross-reference with existing structures** — does it complement or conflict with current mappings?
6. **Document the citation with lane tags** — add to the Citation Matrix with a primary lane and any secondary relevance tags

---

5. Citation Matrix

All citations organized by discipline lane. Each citation has one primary lane and may include secondary relevance tags, reflecting the interdisciplinary nature of the literature. Strict single-lane assignment would be administratively clean but academically dishonest for inherently cross-disciplinary sources.

5.1 PHILOSOPHY OF ANALYSIS

CITATION	DOI	SUPPORTS
Aristotle. *Rhetoric* (c. 350 BCE). Book I, Ch. 2–3.	—	Ethos/Pathos/Logos — Five Perspectives
Aristotle. *Nicomachean Ethics*, Book VI.	—	Phronesis (Executive); Techne (IT Pro)
Vlastos, G. (1983). "The Socratic Elenchus." *OSAP*	—	Socratic verification structure
Benson, H. H. (2011). "Socratic Method." *Cambridge Companion*	—	Elenchus definition and scope
Wilson, J. D. (1987). *ACM SIGCSE*	10.1145/31726.31755	Socratic method in CS
Chidambaram, S. et al. (2024). *EMNLP Findings*	10.18653/v1/2024.findings-emnlp.908	Socratic feedback in code generation
Krishnamurthy, B. et al. (2011). *Computer Communications*	10.1016/j.comcom.2010.09.014	Socratic validation in networking +PROTOCOL SCIENCE
Rife, M. C. (2010). *IEEE Trans. Prof. Comm.*	10.1109/TPC.2010.2052856	Aristotelian rhetoric in digital tools
Arrichiello, V. (2016). *INCOSE*	10.1002/j.2334-5837.2016.00263.x	Phronesis in systems engineering
Alderman, C. (2018). *J. Pharmacy Practice*	10.1002/jppr.1468	Aristotelian framework in practice +HUMAN FACTORS
Malik, A. et al. (2020). *Health Care Analysis*	10.1007/s10728-020-00398-7	Phronesis as professional virtue

Hylving, L. & Koutsikouri, D. (2016). *HICSS*	10.1109/HICSS.2016.574	Phronesis in digital innovation +HUMAN FACTORS
Goldkuhl, G. (2012). *EJIS*	10.1057/ejis.2011.54	Philosophical frameworks in IS research
Cataloging & Classification Quarterly (2009)	10.1080/01639370903111981	Aristotelian categories applied to IT

5.2 HUMAN FACTORS

CITATION	DOI	SUPPORTS
Johnston, A. et al. (2023). *Computers & Security*	10.1016/j.cose.2022.103020	Rhetorical validity in security communication +PHILOSOPHY
Johnston, A. C. & Warkentin, M. (2010). *MIS Quarterly*	10.2307/25750691	Pathos-driven security motivation
Boss, S. R. et al. (2015). *MIS Quarterly*	10.25300/MISQ/2015/39.4.5	Fear appeals and protective security behaviors
van Bavel, R. et al. (2019). *IJHCS*	10.1016/j.ijhcs.2018.11.003	Protection motivation in security nudge design
Benabdallah, G. & Peek, N. (2024). *CHI EA*	10.1145/3613904.3642720	Technical mentality in HCI practice +PHILOSOPHY
Gray, C. M. et al. (2024). *ACM J. Responsible Computing*	10.1145/3656468	Ethics in technology practice +PHILOSOPHY

5.3 PROTOCOL SCIENCE

Protocol science citations are documented in the primary methodology document. See “DNS Tool: Confidence-Scored Analysis of Domain Security Infrastructure,” Section 8 (References) for the complete RFC and ICD 203 citation list. They are not duplicated here to maintain lane separation.

5.4 HUMAN FACTORS Scotopic Interface Design

DNS Tool's Covert Recon Mode uses a scotopic-informed red-spectrum interface designed to preserve dark adaptation for operators working in low-light environments. The design is grounded in established vision science:

- Hecht, S. & Hsia, Y. (1945). "Dark adaptation following light adaptation to red and white lights." *J. Opt. Soc. Am.*, 35(4). DOI: 10.1364/JOSA.35.000261 — Demonstrates that red light preserves rod sensitivity during dark adaptation.
- Miles, W. R. (1953). "Red goggles for producing dark adaptation." *J. Opt. Soc. Am.*, 43(4). DOI: 10.1364/JOSA.43.000435 — Confirms the effectiveness of red-filtered environments for maintaining scotopic sensitivity.
- CIE scotopic luminous efficiency function V′(λ), CIE dataset DOI: 10.25039/cie.ds.gr6w4b5g

Military standards informing the design: MIL-STD-3009 (NVIS radiance compatibility for cockpit displays) and MIL-STD-1472H (human engineering design criteria for military systems).

Hardware Limitation Disclosure

Consumer RGB displays cannot produce true scotopic-compliant output. Standard LCD and OLED panels use RGB subpixel arrays that emit across the visible spectrum, including wavelengths that stimulate rod cells and degrade dark adaptation. Achieving full scotopic compliance requires NVIS-compatible display hardware (e.g., military-grade cockpit displays with narrow-band red phosphors or filtered backlight systems).

DNS Tool's current implementation is therefore a **scotopic-informed approximation on consumer RGB hardware**. The red-spectrum palette minimizes blue-light emission and reduces rod stimulation relative to conventional dark-theme interfaces, but cannot achieve the spectral purity of NVIS-compliant systems. This is an explicit research goal: the platform is designed so that operators on NVIS-compatible hardware would experience a display environment meeting MIL-STD-3009 radiance requirements, while operators on consumer hardware receive the best available approximation within the physical constraints of their display technology.

The color palette selection reflects years of iterative refinement seeking 3–5 colors that maintain readability, semantic distinction, and visual hierarchy within the red-spectrum constraints imposed by scotopic design principles.

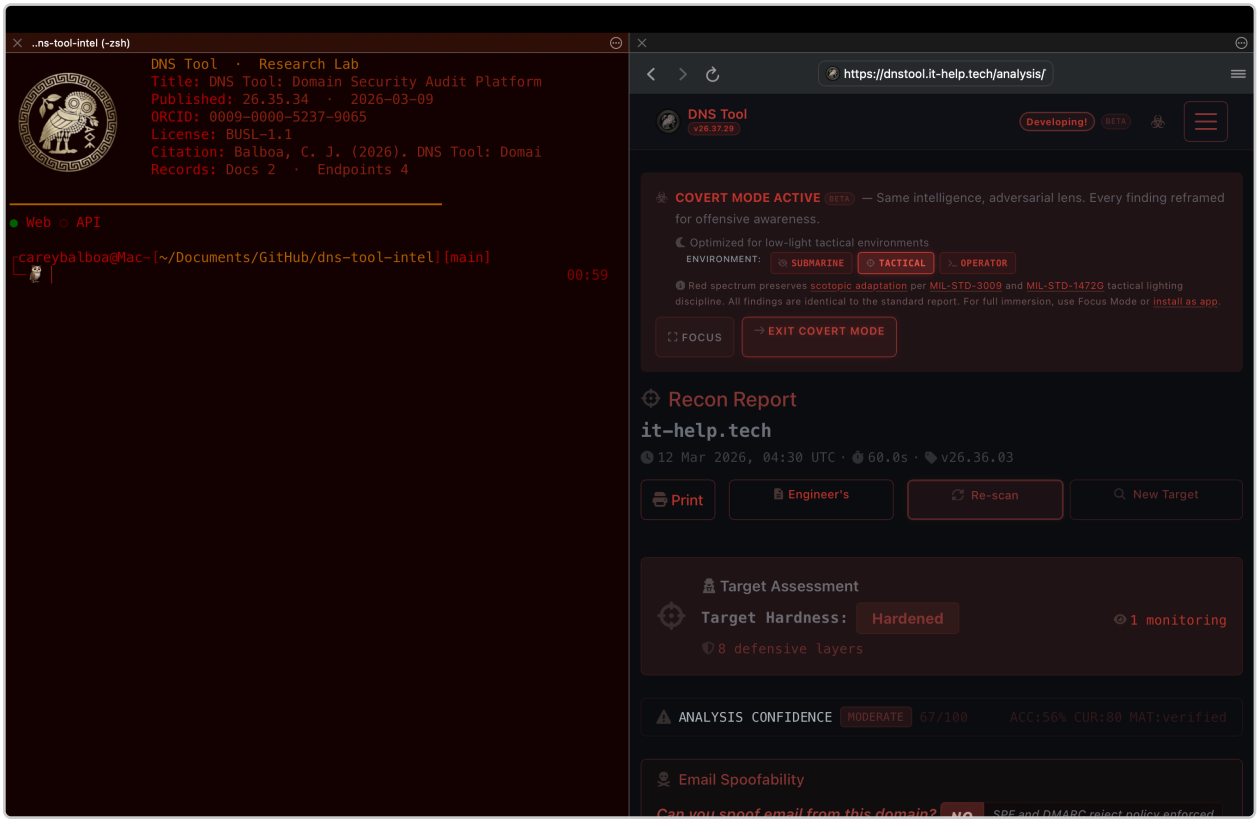


Figure 1. *The author's scotopic-informed workspace in daily operational use. Left: terminal environment with red-spectrum color scheme. Right: DNS Tool Covert Recon Mode displaying a live analysis in the scotopic-optimized interface. Both environments use the same scotopic-informed palette to minimize rod-cell stimulation on consumer RGB hardware. This configuration represents the practical implementation of the design principles described in this section — a working environment optimized for extended screen exposure during security analysis operations.*

5.5 HUMAN FACTORS Live Topology Visualization

During analysis, DNS Tool presents a live protocol/workflow topology that shows DNS resolution unfolding in real time — not a simulated loading animation, but actual phase-by-phase progress through the multi-resolver analysis pipeline. This design serves multiple human-factors objectives supported by peer-reviewed research:

Perceived performance and uncertainty reduction:

- Myers, B. A. (1985). "The importance of percent-done progress indicators for computer-human interfaces." *CHI '85*. DOI: 10.1145/317456.317459 — Progress indicators reduce perceived duration and user anxiety.
- Nah, F. F.-H. (2004). "A study on tolerable waiting time." *Behaviour & Information Technology*, 23(3). DOI: 10.1080/01449290410001669914 — Meaningful feedback during waits extends user tolerance thresholds.

- Harrison, C. et al. (2010). "Faster Progress Bars: Manipulating Perceived Duration with Visual Augmentations." *CHI '10*. DOI: 10.1145/1753326.1753556

Mental model formation through process visualization:

- Hundhausen, C. D. et al. (2002). "A meta-study of algorithm visualization effectiveness." *J. Visual Languages & Computing*, 13(3). DOI: 10.1006/jvlc.2002.0237 — Dynamic process visualization supports cognitive engagement and comprehension of system behavior.
- Shaffer, C. A. et al. (2010). "Algorithm visualization: the state of the field." *ACM Trans. Computing Education*, 10(3). DOI: 10.1145/1821996.1821997

Transparency and trust in automated analysis:

- Dzindolet, M. T. et al. (2003). "The role of trust in automation reliance." *Int. J. Human-Computer Studies*, 58(6). DOI: 10.1016/S1071-5819(03)00038-7 — Users calibrate trust more accurately when they can observe the automated process operating.

The topology visualization bridges the gap between the abstraction of DNS infrastructure and human understanding by making protocol behavior observable. Users do not merely receive results — they watch multi-resolver consensus form, see DNSSEC validation chains resolve, and observe the analysis pipeline traversing protocol-specific evaluation stages. This transforms a passive waiting experience into an active learning opportunity, serving both the educational mission and the transparency commitment documented in the Socratic verification workflow (Section 2).

---

6. Precedent and Positioning

6.1 What We Can Say

Based on review of publicly available OSINT security tool documentation, methodology papers, and academic literature on security tool design, the formal application of classical philosophical frameworks (Socratic elenchus, Aristotelian analytical categories) to security analysis communication — with lane-separated academic citations — appears uncommon in the domain security and OSINT tooling space.

6.2 What We Cannot Say

We have not conducted a systematic literature review (SLR) sufficient to claim "first" or "only." The absence of found precedent is not proof of absence. If a systematic review is conducted in the future and confirms the claim, it can be stated with appropriate citation to that review.

6.3 What the Work Demonstrates

The work demonstrates that classical analytical structures can be applied to security intelligence communication without compromising protocol science — provided the disciplinary lanes remain separated, citations remain verifiable, and no philosophical claim is treated as protocol evidence.

---

7. Relationship to Primary Methodology

This document is a companion to “DNS Tool: Confidence-Scored Analysis of Domain Security Infrastructure” (Balboa, 2026). The primary methodology document addresses data collection, analysis methodology, confidence scoring, and epistemic correction — all within the Protocol Science lane.

This companion document addresses why the analysis is structured into five perspectives (Philosophy of Analysis), why verification commands follow a Socratic pattern (Philosophy of Analysis), how communication structure accounts for multiple professional contexts (Human Factors), and how narrative architecture is maintained as infrastructure (Philosophy of Analysis).

Neither document modifies the other. Protocol science findings are determined by RFC compliance and resolver evidence. Philosophical foundations explain the *communication architecture* through which those findings reach human decision-makers.

Citation

```
@misc{balboa2026philfound,
  author       = {Balboa, Carey James},
  title        = {Philosophical Foundations for Security Analysis Communication},
  year         = {2026},
  note         = {Companion to DNS Tool Methodology (DOI: 10.5281/
zenodo.19468134)},
  url          = {https://dnstool.it-help.tech/foundations}
}
```

OWL SEMAPHORE SYSTEM — CLASSIFICATION LEDGER



NORMATIVE

$T = I$ $\det = +1$

$(x, y) \to (x, y)$

"This is the standard."

RFC 2119 MUST / SHALL



NON-NORMATIVE

$T = \sigma_v$ $\det = -1$

$(x, y) \to (-x, y)$

"This reflects the standard."

Informative / Advisory (NOTE)



CRITICAL

$T = C_2$ $\det = +1$

$(x, y) \to (-x, -y)$

"This inverts the standard."

RFC 2119 MUST NOT / SHALL NOT



METACOGNITIVE

$T = \sigma_h$ $\det = -1$

$(x, y) \to (x, -y)$

"This audits the standard."

Observer audit / Frame inversion

KLEIN FOUR-GROUP V_4 — CLOSURE IN O(2)

$I \cdot \sigma_v \cdot C_2 \cdot \sigma_h$ | $\sigma \circ \sigma = I$ · $C_2 = \sigma_v \circ \sigma_h$ · Every element is its own inverse

---

DNS Tool v26.51.0 · dnstool.it-help.tech · DOI: 10.5281/zenodo.19468134

Related documents: Methodology Paper · Founder's Manifesto · Communication Standards · Reference Library · Sources & Citations

© 2024–2026 IT Help San Diego Inc. · Licensed under BUSL-1.1