HotRFC PROPOSAL

AIDNS: Measuring Security and Stability Impacts of AI on the DNS Root at IETF 126 Vienna

Olorundare, James Kunle, SMIEEE

Email: olorundarek@gmail.com | WhatsApp: +2348036551591

IRTF HOTRFC SESSION | JULY 2026

AIDNS

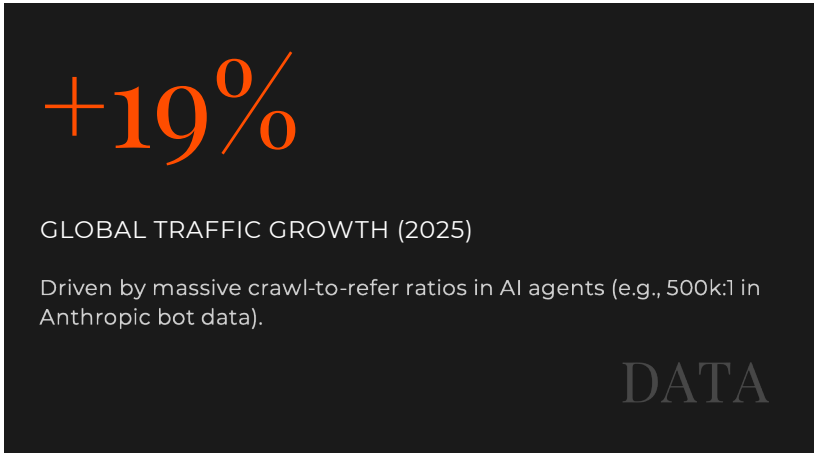
IRTF RESEARCH GROUP

The Paradigm Shift: Human to "Synthetic" Traffic

The DNS was historically designed for human-centric browsing patterns. However, we are witnessing a fundamental transition to autonomous **"Agentic"** behaviors.

AI-powered applications now perform high-frequency automated web retrieval and API calls, generating distinctive DNS query behaviors that current technical tools fail to quantify.

> *"Current traffic models are predicated on human-driven browsing; AI is breaking that mold."*



The Caching Paradox & Root Stability

TRADITIONAL TRAFFIC

Human Interaction

High cache efficiency (>90% resolved at edge)

Stable TTL records for reuse

Protects core infrastructure from volume

AGENTIC TRAFFIC

AI Agent Interaction

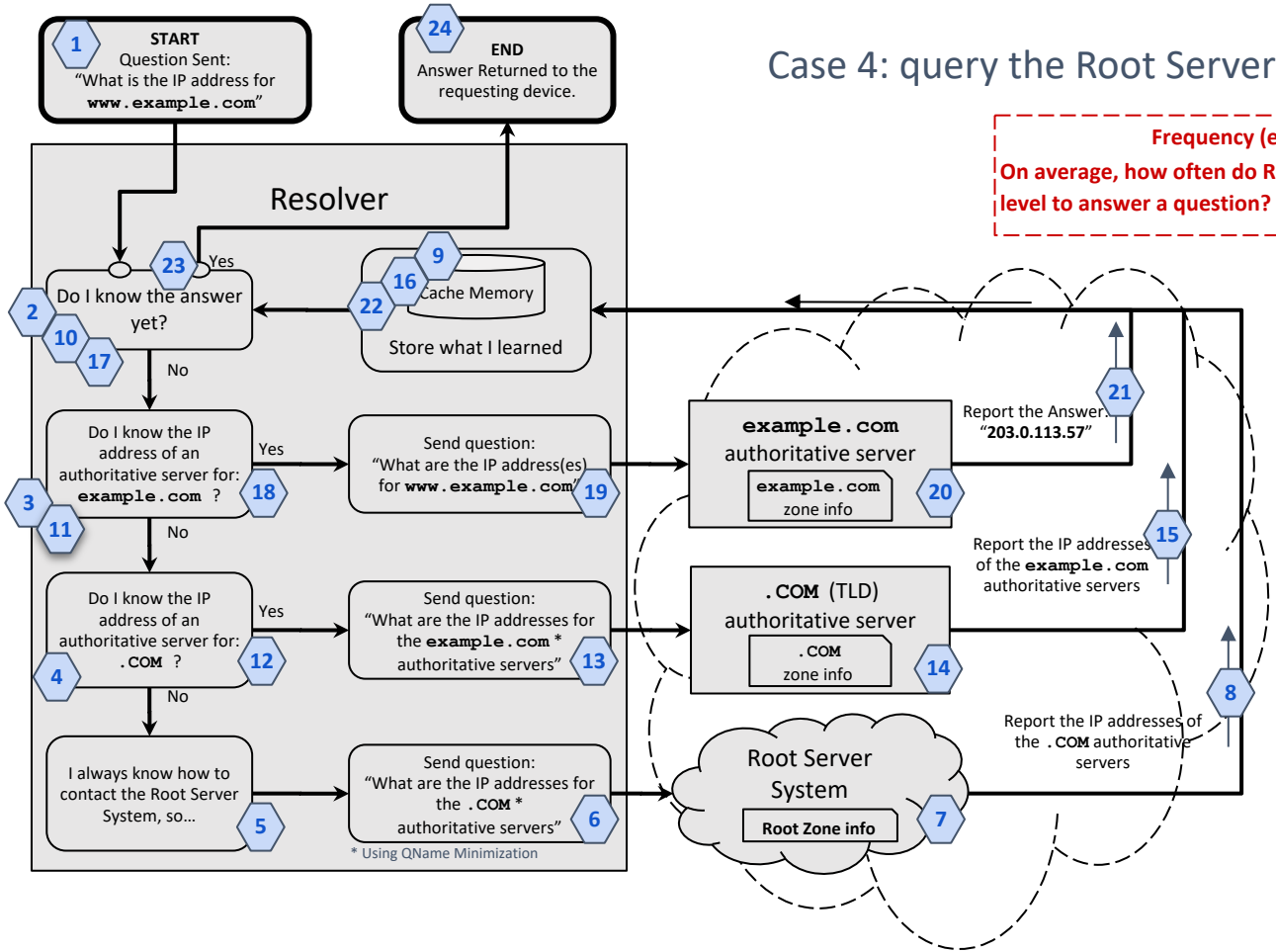
"Cache-Shattering" behaviors

Short TTL demands for real-time updates

Direct Root Access: Bypassing local resolvers

RESULT: Novel stressors on Root Server Operators (RSOs)

Case 4: query the Root Server System



Frequency (estimates):

On average, how often do Resolvers consult at this level to answer a question?

Routine:

> 90% of answers are returned needing cache memory only

Occasional:

~ 5% of answers require a question to the domain name's authoritative server

Uncommon:

~ 2% of answers require a question to the TLD authoritative server

Rare:

~ 0.02% of answers require a question to the RSS

Strategic Objective: Focused Root Stability

PRIMARY GOAL

Investigate the security and stability impacts of AI on the DNS Root Service System—the most critical point of failure in the Internet's naming architecture.

ROOT

KEY RESEARCH QUESTIONS

Autonomous Stressors

How do autonomous agents introduce novel stressors that threaten the resilience of Root Server Operators (RSOs)?

Cache-Busting Resilience

What is the systemic impact of "cache-busting" AI behaviors on global resolution latency and root query volume?

The Roadmap: Form, Study, then Build

01

RG/BoF FORMATION

- Establish the AI and DNS Interactions (AIDNS) Research Group.
- Foster multi-disciplinary collaboration: Network Engineers + AI Researchers.

02

EMPIRICAL STUDY

- Conduct longitudinal study of DNS telemetry.
- Gather pragmatic evidence of AI-driven traffic patterns.

03

HACKATHON BUILD

- Launch IRTF Hackathon project post-formation.
- Prototype open-source measurement toolkit for the community.

The "AIDNS" Measurement Toolkit

Classification Heuristics

Advanced algorithms to distinguish between human-driven and AI-generated DNS traffic patterns in real-time.

Behavioral Intent

Deep analysis of query structures to identify "Agentic" behaviors and potential cache-busting strategies.

Lightweight Instrumentation

Open-source, low-overhead measurement probes designed for deployment across diverse Root Server environments.

Telemetry Aggregation

Standardized data collection formats to foster cross-disciplinary research and longitudinal studies.

PRIMARY OBJECTIVE

Provide the technical community with the visibility required to secure the Root against evolving synthetic workloads.

Why This Matters for the IRTF

Evidence-Based Defense

The emergence of "Offensive AI" requires a defense grounded in data. We move the conversation from speculation to pragmatic, longitudinal telemetry.

Systematic Measurement

Providing the foundation for systematic measurement of AI's interaction with core infrastructure, ensuring a "fit-for-purpose" advisory framework.

Protocol Optimization

Our findings will inform future protocol enhancements (e.g., SVCB or DNS-AID), ensuring they are optimized for sub-second, machine-driven execution.

Architectural Stability

Ensuring the DNS ecosystem remains resilient. Strategic resilience is the foundation of the AI-driven digital economy and global connectivity.

Join the AIDNS Research Group

THE PROBLEM

AI agents are fundamentally changing DNS traffic patterns, creating potential instability at the Root that our current models cannot quantify.

THE SOLUTION

An IRTF Research Group dedicated to the empirical measurement and systematic study of these machine-driven interactions.

Next Steps

- Join the BoF to define the research methodology and goals.
- Collaborate on the longitudinal telemetry study of DNS traffic.
- Participate in the Hackathon to build the measurement toolkit.

Olorundare, James Kunle

PROPONENT | AIDNS BOF

Thank you

The End

Contact details:

Olorundare, James Kunle, SMIEEE

Email: olorundarek@gmail.com |

WhatsApp: +2348036551591

References

ICANN COMMUNITY FORUM (2026)

“ RSSAC Overview at ICANN 85 New Commers Session”

AKAMAI (2025)

"Your AI Strategy Is Only as Strong as Your DNS: Strengthening Posture Management."

NOKIA (2025)

"DDoS in 2025: The Year Automation Took the Wheel - Multi-Vector Strike Analysis."

IETF RFC 9460

"Service Binding and Parameter Priority Settings in DNS (SVCB and HTTPS Resource Records)."

MICROSOFT (2025)

"Digital Defense Report: Rising AI-Driven Threats and the Rethink of Traditional Defenses."

DNSFILTER (2025)

"Annual Security Report: AI-Driven Cyberattacks and Threat Traffic Trends."

EFFICIENTIP (2024)

"The Importance of DNS Security in the AI-Driven Digital Age: Real-Life Vulnerabilities."

CYBER DEFENSE MAGAZINE (2026)

"AI Vs. AI: Making AI Part of Your DNS Security Arsenal Against Evolving Threats."