AdBlock via DNS

Personal Information

- **Name:** Hazem Hamdi Mahmoud Abdelqader
- **University:** Nahda University (NUB)
- **Faculty:** Faculty of Engineering
- **Department:** Communications and Electronics Engineering

- **Submission Date:** February 16, 2026

Contact Details

- **Phone:** +20 106 238 6571
- **Email:** hazemhamdypersonal@gmail.com
- **GitHub:** github.com/Hazem-Hamd

Professional Qualifications & Training

Language Proficiency

- **English (CEFR Level: B2/C1 equivalent):** Score **403** – Certified by the **American University in Cairo (AUC)**.

Technical Certifications

Program	Provider
CCNA	CISCO
Mobile Communication	WE (Telecom Egypt)
Fiber Optic	WE (Telecom Egypt)
Retail Technical Network	WE (Telecom Egypt)

Analysis of DNS Server 94.140.14.14

1. Provider Identification

- **Owner: AdGuard Software Ltd.**
- **Service Name:** AdGuard DNS (Default/Non-Filtering Server).
- **Location:** Anycast network (Global nodes, frequently routed through European data centers).
- **Protocol Support:** Standard DNS (Port 53), DNS-over-HTTPS (DoH), and DNS-over-TLS (DoT).

---

2. Core Functionality

The IP 94.140.14.14 serves as a **Recursive DNS Resolver**. When you configure this IP on your router or PC, it acts as the "phonebook" for your internet connection.

Key Features:

- **Ad & Tracker Blocking:** It automatically intercepts and blocks requests to known advertising servers and tracking scripts at the DNS level.
- **Malware Protection:** It prevents your device from connecting to domains recognized for hosting phishing content or malware.
- **Privacy Enhancement:** Unlike ISP-provided DNS servers, AdGuard does not sell your browsing history to third-party advertisers.

---

3. How it Works (The Sinkhole Mechanism)

When a website tries to load an ad from a domain like ads.example.com, the following happens:

1. Your device asks **94.140.14.14**: "What is the IP for ads.example.com?"
2. The server checks its **Blocklist**.
3. Since the domain is a well-known ad provider, the server returns 0.0.0.0 (a "Sinkhole") instead of the real IP.
4. The ad fails to load, but the rest of the website loads faster and cleaner.

---

4. Technical Comparison

AdGuard provides different IPs based on the user's needs. Here is where **94.140.14.14** fits:

Server Type	Primary IP	Function
Default	**94.140.14.14**	Blocks Ads, Trackers, and Malware.
Family Protection	**94.140.14.15**	Blocks Ads + Malware + Adult Content (Safe Search).
Non-Filtering	**94.140.14.140**	Pure DNS resolution with no blocking.

here are two main ways to distribute DNS

1. Router Level (Network-Wide Distribution)

This is the most effective method for home users because it covers every device connected to the Wi-Fi (Smart TVs, Guest Phones, Laptops) without manual setup on each one.

- **How it works: You change the DNS settings in the DHCP Server settings of your Home Gateway (e.g., Huawei or ZTE router).**
- **Configuration:**
    1. **Access your router page (usually 192.168.1.1).**
    2. **Navigate to LAN -> DHCP Server.**
    3. **Set Primary DNS to 94.140.14.14 and Secondary DNS to 94.140.14.14.**
- **Best for: Saving bandwidth for the whole family and blocking ads on devices that don't have settings (like Smart TVs).**

---

2. Mobile Level (Private DNS / DNS-over-TLS)

This method is specific to the smartphone and is highly recommended for personal privacy. It works on both Wi-Fi and Mobile Data (4G/5G).

A. Android (Version 9+)

Android uses DoT (DNS over TLS) which encrypts your DNS queries.

1. **Go to Settings > Network & Internet > Private DNS.**
2. **Select Private DNS provider hostname.**
3. **Enter: 94.140.14.14**
4. **Hit Save.**

B. iOS (iPhone)

iOS requires a DNS Profile or a third-party app (like the AdGuard app) to change the system-wide DNS.

1. **Download the configuration profile from the official AdGuard site.**
2. **Go to Settings > General > VPN & Device Management.**
3. **Install and trust the profile.**

DNS Security Risks & Vulnerabilities

Data Centralization: Using a third-party DNS shifts your entire browsing history from your ISP to a single provider, creating a privacy risk if their logs are ever leaked or sold.

Spoofing & Poisoning: Compromised DNS servers can redirect traffic to phishing sites. Using encrypted protocols like **DoH** or **DoT** is essential to mitigate this by verifying server identities.

Single Point of Failure: If your primary DNS provider goes down, your internet connectivity effectively breaks. Reliability requires configuring a **Secondary DNS** from a different provider for redundancy.

False Positives: Over-aggressive blacklisting can block legitimate domains, leading to "broken" apps or websites and making troubleshooting significantly more difficult.

Limited Protection: DNS filtering only operates at the domain level. It cannot inspect content or block "in-stream" threats (like YouTube ads), meaning it is not a substitute for **Layer 7** security.