CDN Detection Methods Summary

The script uses **5 detection methods** ranked by reliability:

---

1. ASN Lookup 🎯

- **Reliability:** 95% (Highest)
- **How:** Queries `whois` to find who owns the IP address
- **Example:** IP `23.50.227.98` → `AS20940` → Akamai Technologies
- **Why reliable:** Authoritative registry data, can't be hidden or faked
- **Covers:** ALL IPs owned by a CDN, not just known ranges

---

2. Reverse DNS (PTR) 🔍

- **Reliability:** 85%
- **How:** Looks up the hostname associated with an IP
- **Example:** `23.50.227.98` → `a23-50-227-98.deploy.akamaitechnologies.com`
- **Why reliable:** Difficult to hide, reveals CDN infrastructure
- **Limitation:** Some IPs may not have PTR records

---

3. CNAME Chain Analysis 🔗

- **Reliability:** 80%
- **How:** Follows DNS alias redirects to find CDN patterns
- **Example:** `cigna.com` → `www.cigna.com.edgekey.net` (Akamai)
- **Patterns detected:** `akadns`, `edgesuite`, `cloudfront.net`, etc.
- **Limitation:** Direct A records skip CNAMEs entirely

---

4. HTTP Headers 📋

- **Reliability:** 70%
- **How:** Examines response headers from HTTP requests
- **Example:** `X-Akamai-Session-Info`, `CF-Ray`, `X-Amz-Cf-Id`
- **Why less reliable:** Many sites strip identifying headers for security
- **Limitation:** Easily hidden or removed by configuration

---

5. IP Prefix Matching 📡

- **Reliability:** 40% (Lowest)
- **How:** Checks if IP starts with known CDN prefixes
- **Example:** `104.16.x.x` → Cloudflare, `23.50.x.x` → Akamai
- **Why less reliable:**
  - Impossible to hardcode all IP ranges
  - Ranges change over time
  - Can miss legitimate CDN IPs
- **Coverage:** Script has 100+ Akamai prefixes (vs 20 in original)

Detection Flow

```
Domain (cigna.com)
  ↓
1. Resolve IPs → [23.50.227.98, ...]
  ↓
2. ASN Lookup ✅ → AS20940 (Akamai) [95% confidence]
  ↓
3. Reverse DNS ✅ → akamaitechnologies.com [85% confidence]
  ↓
4. CNAME Chain ✅ → edgekey.net [80% confidence]
  ↓
5. HTTP Headers ? → May or may not show [70% confidence]
  ↓
6. IP Prefix ✅ → Matches 23.50.x.x [40% confidence]
  ↓
Final Result: Akamai detected with HIGH CONFIDENCE
```

Why Multiple Methods?

Scenario	Methods That Still Work
Headers hidden	ASN, Reverse DNS, CNAME, IP Prefix
No CNAME (direct A record)	ASN, Reverse DNS, Headers, IP Prefix
IP not in prefix list	ASN, Reverse DNS, CNAME, Headers
Everything hidden	ASN still works!

The combination ensures accurate detection even when individual methods fail. The script reports the **highest confidence level** from any successful method.

Quick Reference Table

Method	Reliability	Speed	Can Be Hidden?	Command Used
ASN Lookup	⭐⭐⭐⭐⭐ (95%)	Slow	❌ No	whois
Reverse DNS	⭐⭐⭐⭐ (85%)	Medium	Rarely	dig -x
CNAME Chain	⭐⭐⭐⭐ (80%)	Fast	Rarely	dig CNAME
HTTP Headers	⭐⭐⭐ (70%)	Fast	✅ Yes	curl -I
IP Prefix	⭐⭐ (40%)	Fast	❌ No	String match

Confidence Scoring

The script calculates an overall confidence score based on the **highest reliability method** that successfully detects a CDN:

- **HIGH (80-100%):** Detected via ASN, Reverse DNS, or CNAME
- **MEDIUM (60-79%):** Detected via HTTP Headers
- **LOW (30-59%):** Detected via IP Prefix only
- **VERY LOW (<30%):** Weak or uncertain detection
- **NONE (0%):** No CDN detected by any method

Key Improvements Over Original Script

Original Script	Enhanced Script
IP prefix only (40% reliable)	5 methods including ASN (95% reliable)
~20 Akamai IP prefixes	100+ Akamai IP prefixes
3 CNAME patterns	10+ CNAME patterns per CDN
No confidence scoring	Confidence levels reported
False "Direct/Origin" labels	Honest "Unknown/Not Detected"
Missed cigna.com ❌	Correctly detects cigna.com ✅