

Forum:[Hack Forums](#)

Thread: [\[CYBERSEC SERIES #6/10 \] DNS Explained: What Happens When You Visit A Website](#)

Mastercarder - May 22, 2026, 7:57 pm

[CYBERSEC SERIES #6/10] Understanding DNS Requests & How Your Traffic Actually Gets Routed

What Actually Happens When You Visit A Website?

Most people use the internet every single day without understanding what's happening in the background.

You type:

Code google.com

...and within seconds the website loads.

But behind the scenes, your request travels through multiple systems, DNS resolvers, routers, networks, and servers before reaching its destination.

Understanding this process is important not just for networking, but also for cybersecurity, privacy, OPSEC, traffic analysis, and troubleshooting.

This thread is a beginner-friendly breakdown of how DNS works and how internet traffic actually gets routed.

1. What Is DNS?

DNS (Domain Name System) acts like the internet's phonebook.

Humans remember names like:

Code google.com

But computers communicate using IP addresses such as:

Code 142.250.70.14

DNS translates domain names into IP addresses so your device knows where to connect.

Without DNS, you'd have to manually remember IP addresses for every website you visit.

2. What Happens When You Visit A Website?

When you enter a website into your browser, something like this happens:

Code 1. Browser requests website

2. DNS resolver searches for IP address

3. DNS server responds with matching IP

4. Your device connects to the server

5. Website sends data back to you

All of this usually happens within milliseconds.

3. Your Request Does NOT Travel Directly

One thing many people misunderstand is that your traffic does not instantly jump from your device straight to the website.

Your data usually passes through:

- your router
- your ISP
- multiple gateways
- backbone infrastructure
- routing systems
- the destination server

The path can constantly change depending on:

- traffic congestion
- server load
- routing efficiency
- geographic location

4. Using Traceroute To See Traffic Paths

A useful networking tool is:
Code traceroute
(or Code tracert on Windows)

Example:

Code tracert google.com

This command shows the “hops” your traffic takes before reaching the destination.

You’ll often see:

- your router
- ISP infrastructure
- regional routing systems
- international routing hops

It’s a useful way to visualize how internet traffic actually moves.

5. DNS & Privacy

DNS requests can reveal a lot about browsing activity.

Even if a website uses HTTPS encryption, DNS requests may still expose:

- domains visited

- timing patterns
- browsing behaviour
- connection activity

This is one reason why:

- encrypted DNS
- DNS-over-HTTPS (DoH)
- DNS-over-TLS (DoT)
- VPNs
- public DNS providers

are frequently discussed in cybersecurity and privacy communities.

6. Common DNS & Networking Tools

Some commonly used tools include:

Code ping
nslookup
tracert / traceroute
Wireshark

These are commonly used by:

- network administrators
- analysts
- researchers
- cybersecurity professionals

to troubleshoot and inspect network traffic.

7. Final Thoughts

A lot of cybersecurity starts with understanding how systems communicate.

Before people jump into things like malware analysis, pentesting, or traffic inspection, it's important to first understand:

- how requests move
- how domains resolve
- how systems communicate across networks

Networking fundamentals are one of the most overlooked parts of cybersecurity.

If you have any questions at all feel free to PM me or drop a comment on the thread below!

By MasterCard @ HF

Stay tuned for Part 7 of the series.

Accumulate - May 24, 2026, 9:52 pm

I'm loving these brotha! Keep it up! :D