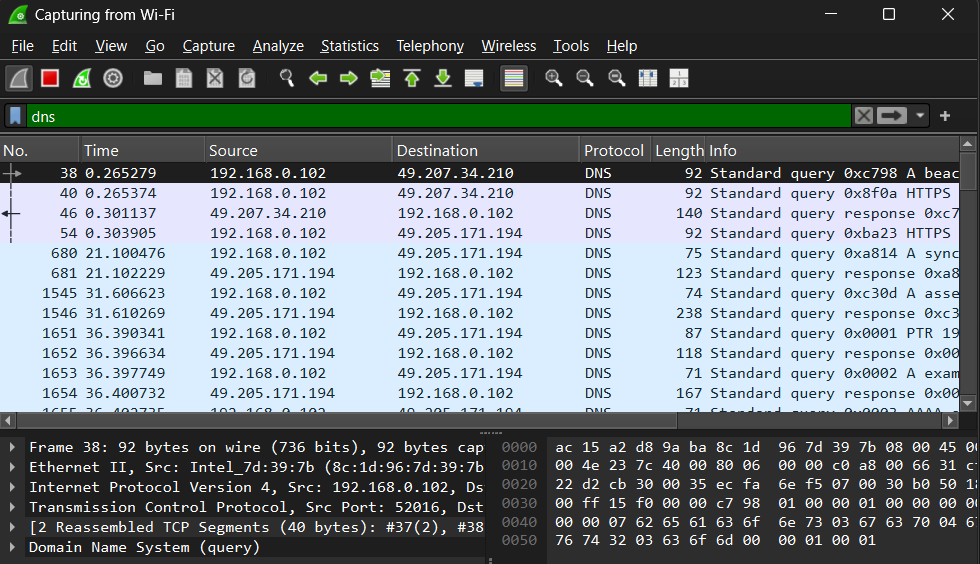
Step 1: **Start Wireshark and Capture DNS Traffic**

1. Open Wireshark.
2. Select your active network interface (Wi-Fi, Ethernet).
3. Click Start Capture.
4. In the Wireshark filter bar, enter:

*dns*

This only displays DNS traffic.

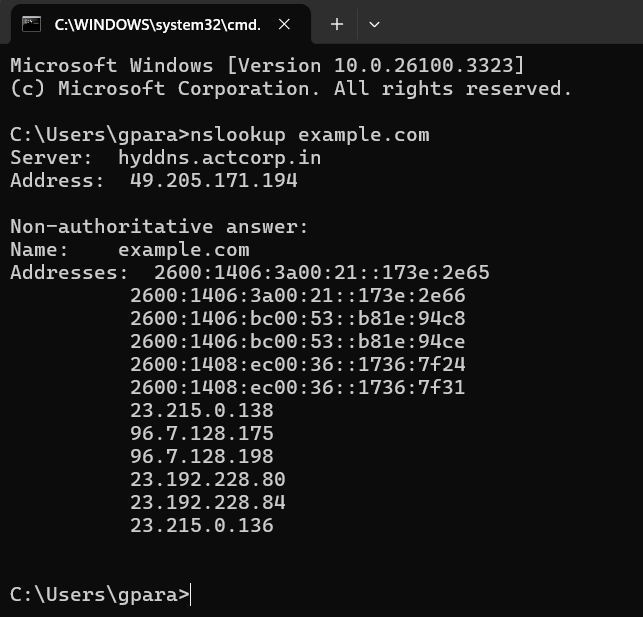


Step 2: **Generate DNS Queries for Testing**

1. Open a command prompt (Windows) or terminal (Linux/macOS).
2. Run the following DNS lookup commands:

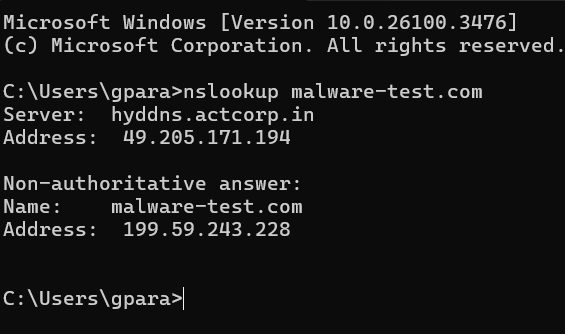
* Using nslookup

*nslookup example.com*



Step 3: **Simulate a query for a known malicious domain**

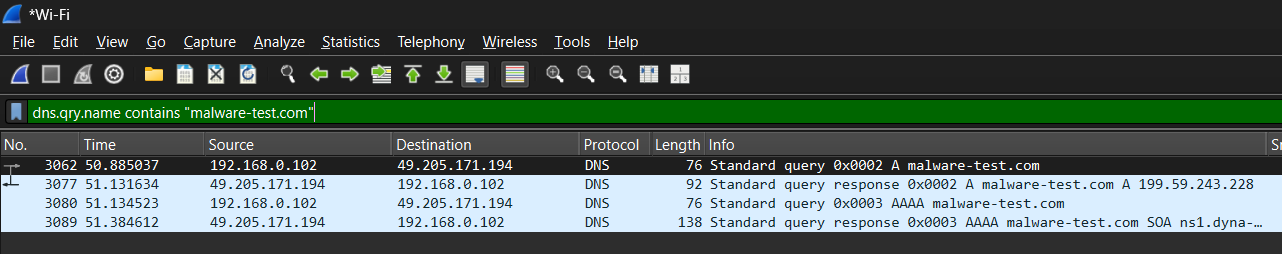
*nslookup malware-test.com*



Step 4 : **Analyze Captured DNS Queries in Wireshark**

1. Stop the Capture after executing the DNS queries.
2. In Wireshark, filter only DNS requests containing malware-test.com:

*dns.qry.name contains “malware-test.com”*

**

To filter all DNS queries containing any request, just filter by entering

*Dns.qry.name*

Step 5 **: Investigate Malicious Domains**

1. Copy any suspicious domains found in Wireshark.
2. Check them on Threat Intelligence Platforms:

* VirusTotal

