Project Title: Deep DNS Enumeration and Analysis with `dig`

Objective:

To perform DNS enumeration and investigate domain configurations using `dig`, a powerful domain information groper tool. This project strengthens analytical skills in understanding how the Domain Name System resolves and distributes information across the internet.

Skills Learned:

- DNS architecture (recursive vs. authoritative)
- Understanding DNS record types (A, NS, MX, SOA)
- Interpreting TTL (Time to Live) and caching behavior
- Root-to-authoritative resolution tracing
- Using CLI tools for domain reconnaissance
- Threat surface evaluation via DNS exposure

Tools Used:

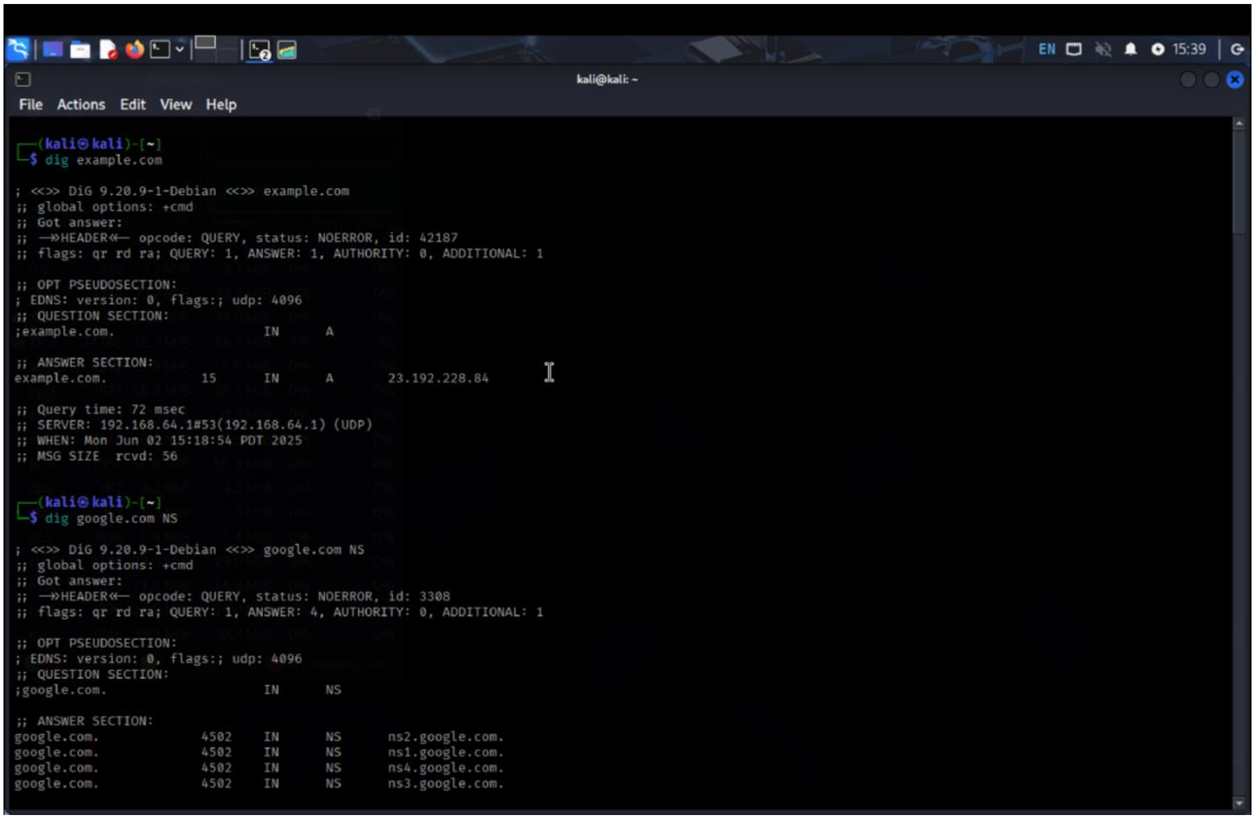
- Kali Linux (or any Unix/Linux terminal)
- `dig` (Domain Information Groper) CLI utility
- Internet connectivity for live DNS queries

Tasks Performed / Steps Executed:

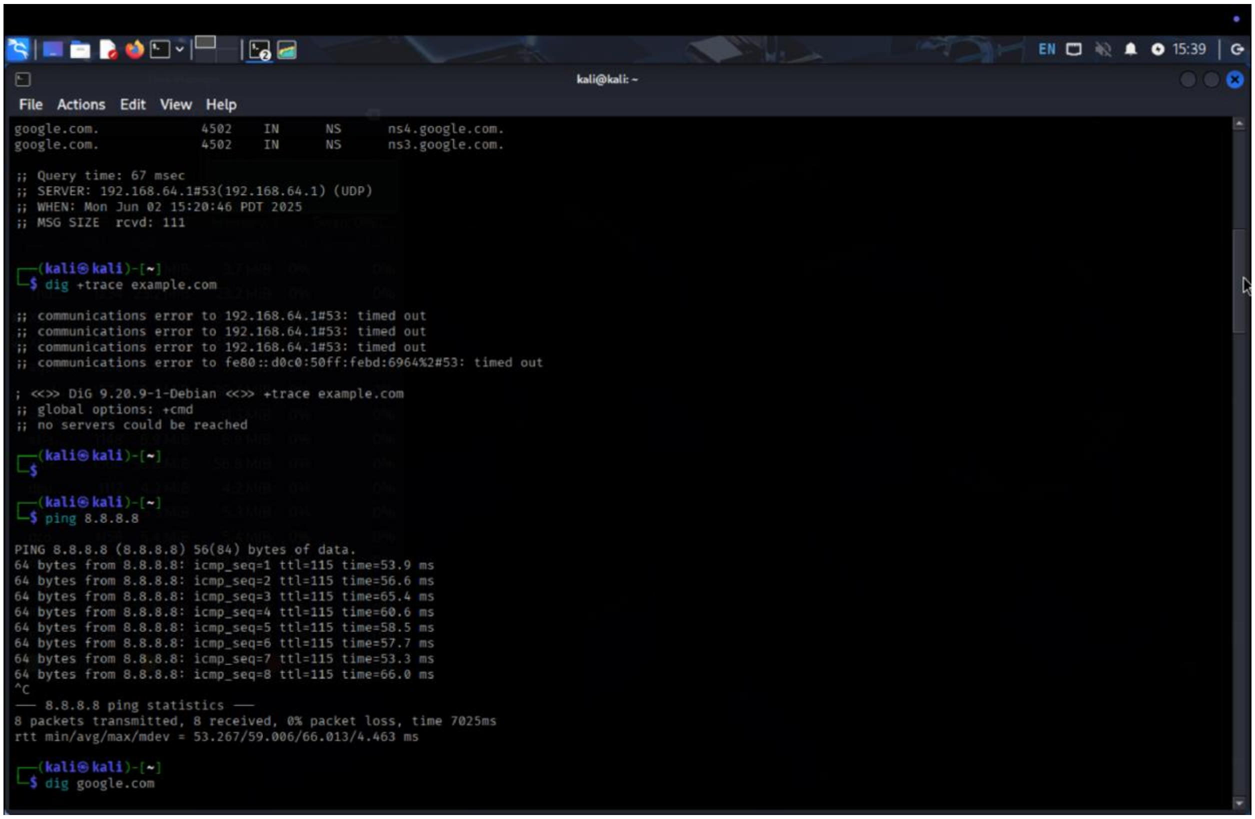
🔍 **Level**	🧪 **Command**	📖 **Description**	✅ **Skills Demonstrated**
🟢 **Basic**	`dig example.com`	Queries A record for `example.com`	Understanding A records & IP resolution
🟡 **Intermediate**	`dig google.com NS`	Retrieves name servers responsible for `google.com`	DNS delegation, understanding NS records
🔴 **Advanced**	`dig +trace openai.com`	Performs full DNS trace from root to authoritative servers	Visualizing full DNS resolution path
🔴 **Advanced**	`dig @8.8.8.8 openai.comdig @1.1.1.1 openai.com`	Compares TTL and DNS responses between Google and Cloudflare servers	TTL analysis, resolver behavior, caching awareness

Real-World Relevance:

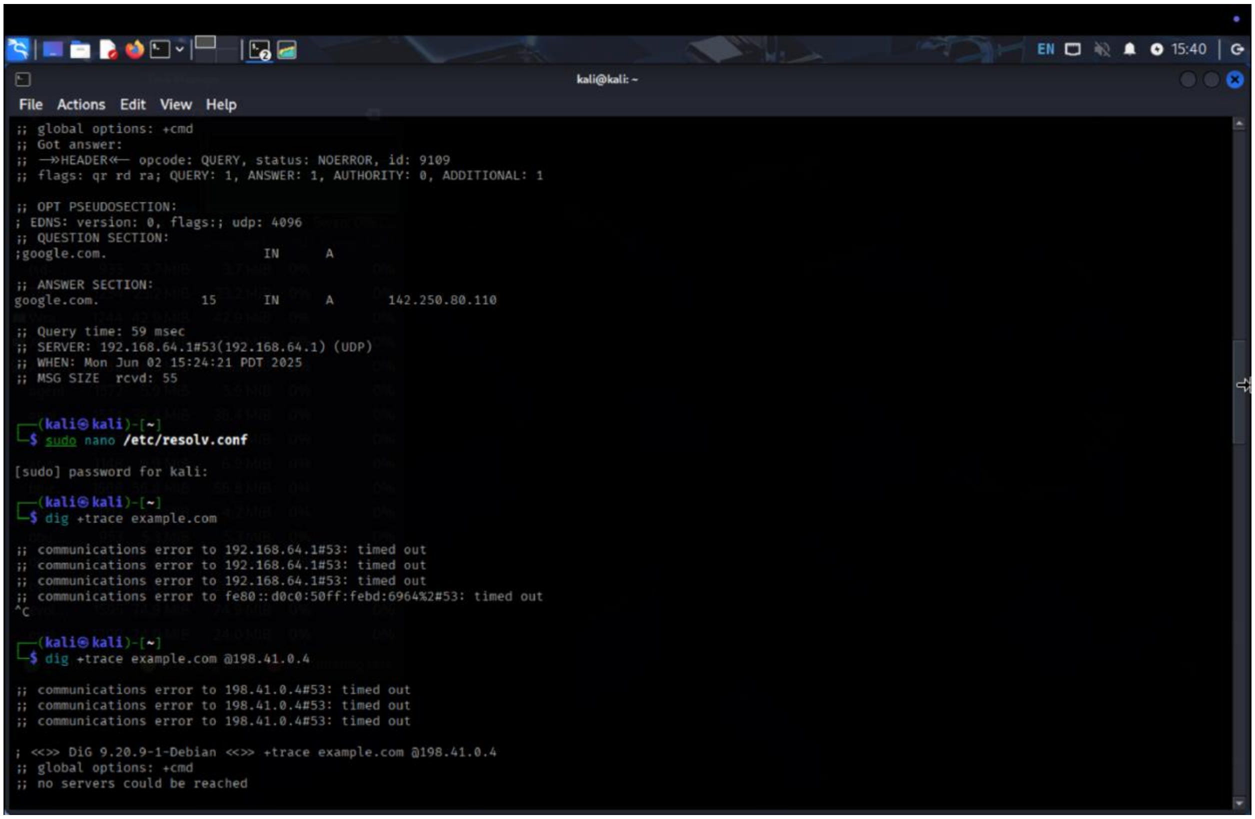
- **Red Team:** Identify DNS misconfigurations that leak internal domains.
- **Blue Team/SOC:** Monitor for unusual TTL changes that might suggest DNS hijacking or poisoning.
- **IT Operations:** Validate live DNS behavior across multiple global resolvers.



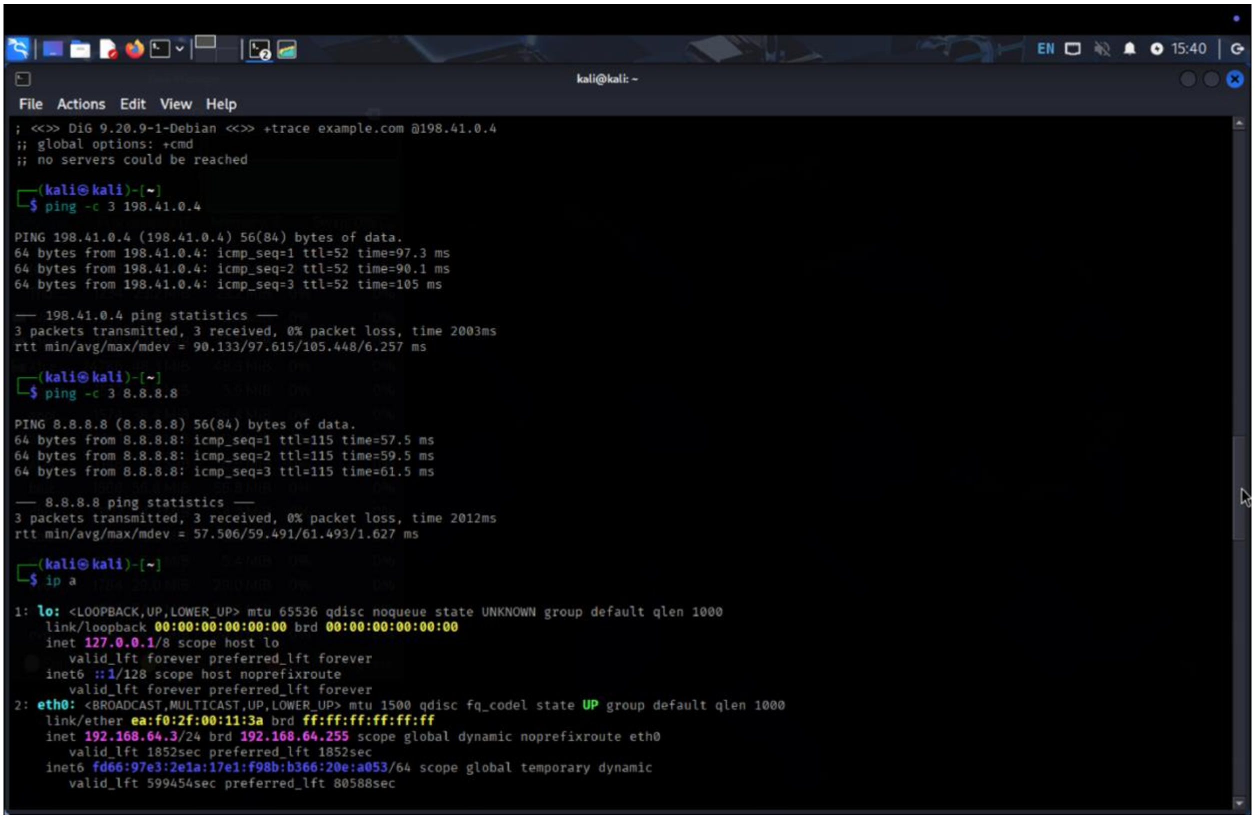
```
┌──(kali㉿kali)-[~]
└─$ dig example.com

; <<>> DiG 9.20.9-1-Debian <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42187
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            15      IN      A       23.192.228.84

;; Query time: 72 msec
;; SERVER: 192.168.64.1#53(192.168.64.1) (UDP)
;; WHEN: Mon Jun 02 15:18:54 PDT 2025
;; MSG SIZE  rcvd: 56


┌──(kali㉿kali)-[~]
└─$ dig google.com NS

; <<>> DiG 9.20.9-1-Debian <<>> google.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3308
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             4502    IN      NS      ns2.google.com.
google.com.             4502    IN      NS      ns1.google.com.
google.com.             4502    IN      NS      ns4.google.com.
google.com.             4502    IN      NS      ns3.google.com.
```



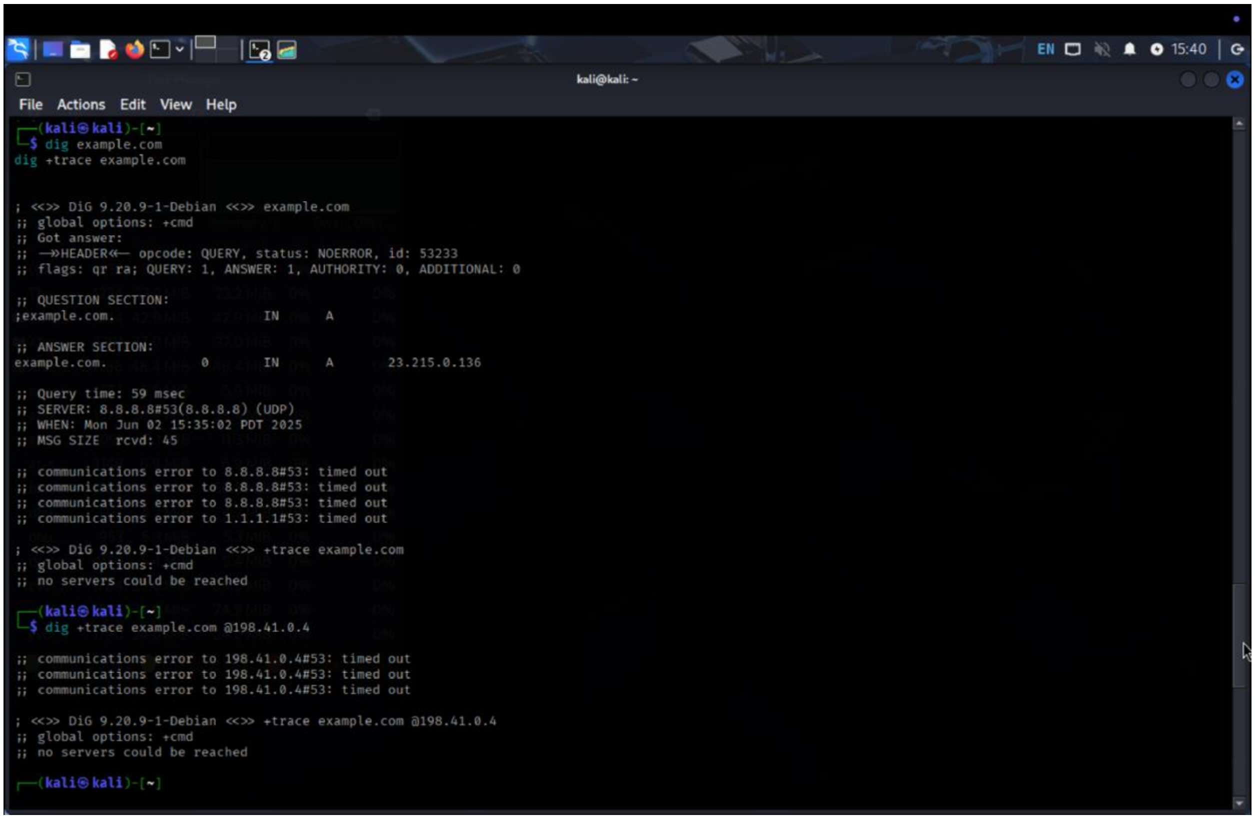
```
google.com.             4502    IN      NS      ns4.google.com.
google.com.             4502    IN      NS      ns3.google.com.

;; Query time: 67 msec
;; SERVER: 192.168.64.1#53(192.168.64.1) (UDP)
;; WHEN: Mon Jun 02 15:20:46 PDT 2025
;; MSG SIZE  rcvd: 111


┌──(kali㉿kali)-[~]
└─$ dig +trace example.com

;; communications error to 192.168.64.1#53: timed out
;; communications error to 192.168.64.1#53: timed out
;; communications error to 192.168.64.1#53: timed out
;; communications error to fe80::d0c0:50ff:febd:6964%2#53: timed out

; <<>> DiG 9.20.9-1-Debian <<>> +trace example.com
;; global options: +cmd
;; no servers could be reached

┌──(kali㉿kali)-[~]
└─$ 

┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=53.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=56.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=65.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=60.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=58.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=57.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=115 time=66.0 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7025ms
rtt min/avg/max/mdev = 53.267/59.006/66.013/4.463 ms

┌──(kali㉿kali)-[~]
└─$ dig google.com
```



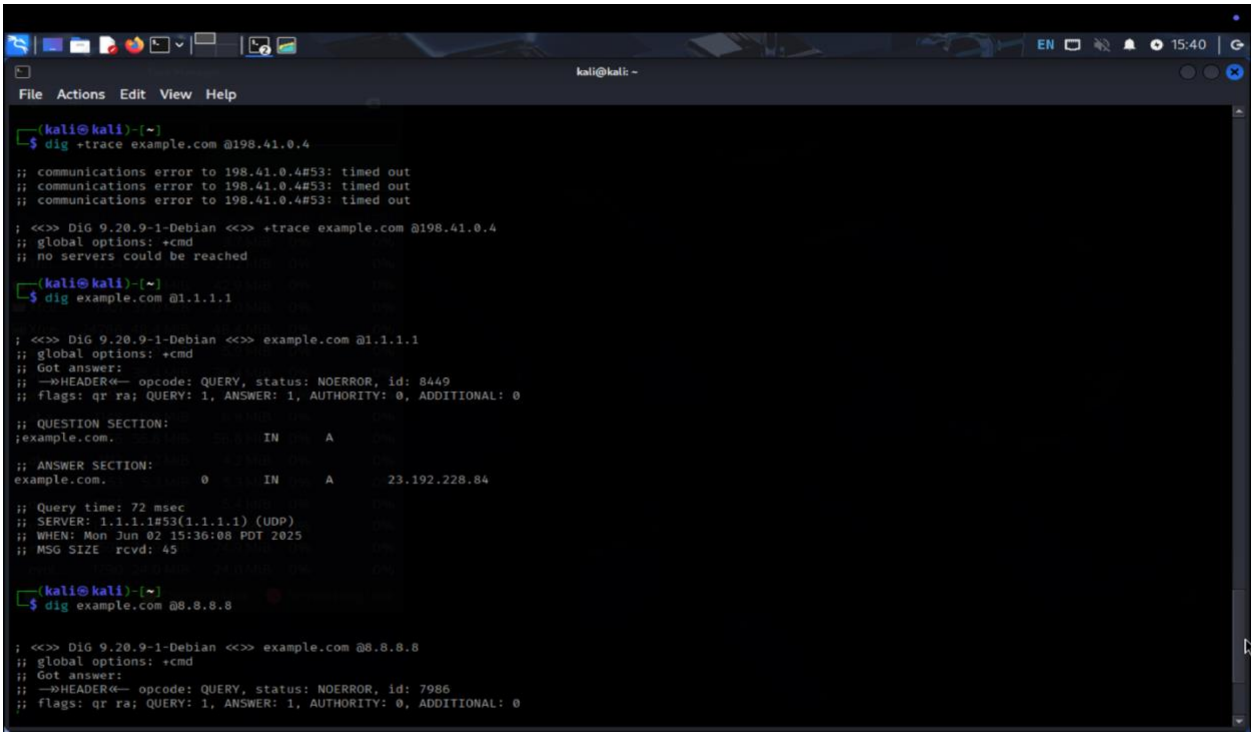
```
;; global options: +cmd
;; Got answer:
;; —»HEADER«— opcode: QUERY, status: NOERROR, id: 9109
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             15      IN      A       142.250.80.110

;; Query time: 59 msec
;; SERVER: 192.168.64.1#53(192.168.64.1) (UDP)
;; WHEN: Mon Jun 02 15:24:21 PDT 2025
;; MSG SIZE  rcvd: 55


┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/resolv.conf

[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ dig +trace example.com

;; communications error to 192.168.64.1#53: timed out
;; communications error to 192.168.64.1#53: timed out
;; communications error to 192.168.64.1#53: timed out
;; communications error to fe80::d0c0:50ff:febd:6964%2#53: timed out
^C

┌──(kali㉿kali)-[~]
└─$ dig +trace example.com @198.41.0.4

;; communications error to 198.41.0.4#53: timed out
;; communications error to 198.41.0.4#53: timed out
;; communications error to 198.41.0.4#53: timed out

; <<>> DiG 9.20.9-1-Debian <<>> +trace example.com @198.41.0.4
;; global options: +cmd
;; no servers could be reached
```



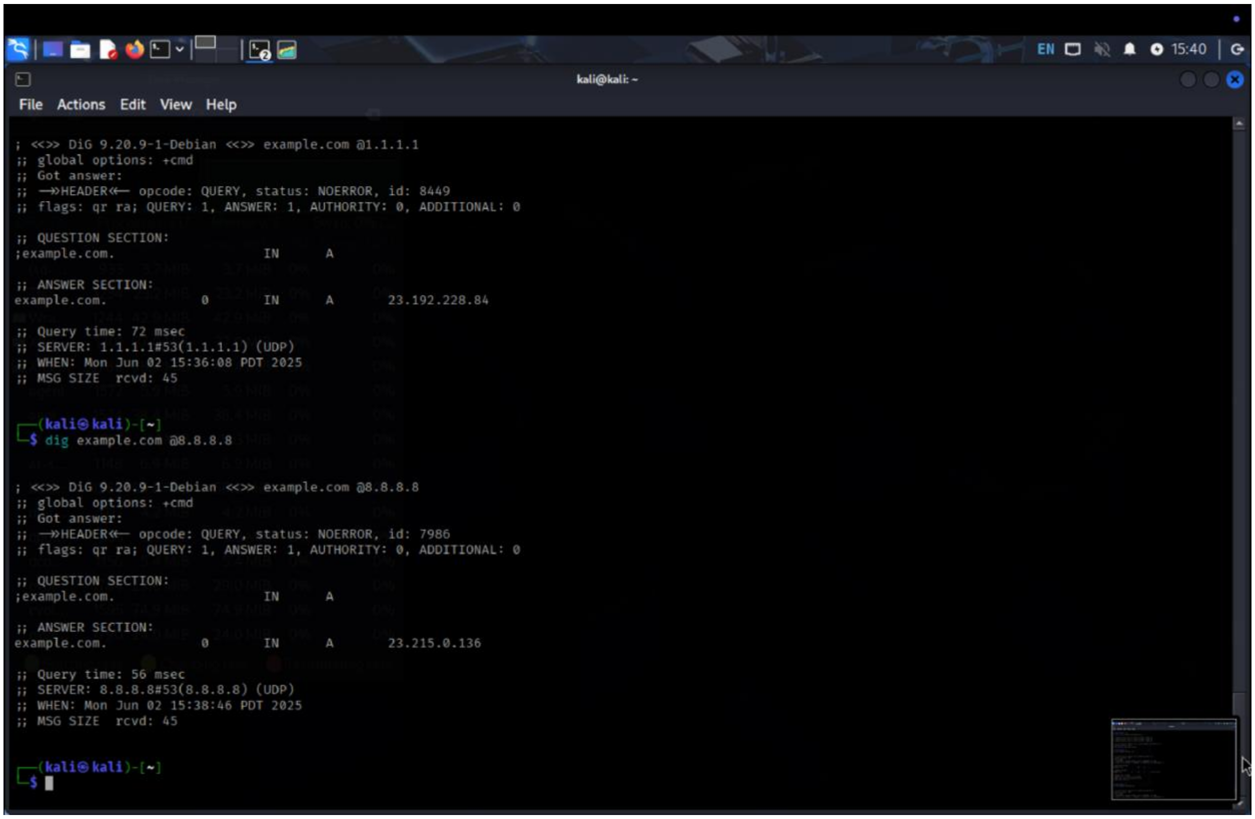
```
; <<>> DiG 9.20.9-1-Debian <<>> +trace example.com @198.41.0.4
;; global options: +cmd
;; no servers could be reached

┌──(kali㉿kali)-[~]
└─$ ping -c 3 198.41.0.4

PING 198.41.0.4 (198.41.0.4) 56(84) bytes of data.
64 bytes from 198.41.0.4: icmp_seq=1 ttl=52 time=97.3 ms
64 bytes from 198.41.0.4: icmp_seq=2 ttl=52 time=90.1 ms
64 bytes from 198.41.0.4: icmp_seq=3 ttl=52 time=105 ms

—— 198.41.0.4 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 90.133/97.615/105.448/6.257 ms

┌──(kali㉿kali)-[~]
└─$ ping -c 3 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=57.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=59.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=61.5 ms

—— 8.8.8.8 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 57.506/59.491/61.493/1.627 ms

┌──(kali㉿kali)-[~]
└─$ ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether ea:f0:2f:00:11:3a brd ff:ff:ff:ff:ff:ff
    inet 192.168.64.3/24 brd 192.168.64.255 scope global dynamic noprefixroute eth0
       valid_lft 1852sec preferred_lft 1852sec
    inet6 fd66:97e3:2e1a:17e1:f98b:b366:20e:a053/64 scope global temporary dynamic
       valid_lft 599454sec preferred_lft 80588sec
```



```
┌──(kali㉿kali)-[~]
└─$ dig example.com
dig +trace example.com


; <<>> DiG 9.20.9-1-Debian <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53233
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            0       IN      A       23.215.0.136

;; Query time: 59 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Jun 02 15:35:02 PDT 2025
;; MSG SIZE  rcvd: 45

;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.8#53: timed out
;; communications error to 1.1.1.1#53: timed out

; <<>> DiG 9.20.9-1-Debian <<>> +trace example.com
;; global options: +cmd
;; no servers could be reached

┌──(kali㉿kali)-[~]
└─$ dig +trace example.com @198.41.0.4

;; communications error to 198.41.0.4#53: timed out
;; communications error to 198.41.0.4#53: timed out
;; communications error to 198.41.0.4#53: timed out

; <<>> DiG 9.20.9-1-Debian <<>> +trace example.com @198.41.0.4
;; global options: +cmd
;; no servers could be reached

┌──(kali㉿kali)-[~]
```



```
┌──(kali㉿kali)-[~]
└─$ dig +trace example.com @198.41.0.4

;; communications error to 198.41.0.4#53: timed out
;; communications error to 198.41.0.4#53: timed out
;; communications error to 198.41.0.4#53: timed out

; <<>> DiG 9.20.9-1-Debian <<>> +trace example.com @198.41.0.4
;; global options: +cmd
;; no servers could be reached

┌──(kali㉿kali)-[~]
└─$ dig example.com @1.1.1.1


; <<>> DiG 9.20.9-1-Debian <<>> example.com @1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8449
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            0       IN      A       23.192.228.84

;; Query time: 72 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Mon Jun 02 15:36:08 PDT 2025
;; MSG SIZE  rcvd: 45

┌──(kali㉿kali)-[~]
└─$ dig example.com @8.8.8.8


; <<>> DiG 9.20.9-1-Debian <<>> example.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7986
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```



```
; <<>> DiG 9.20.9-1-Debian <<>> example.com @1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8449
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            0       IN      A       23.192.228.84

;; Query time: 72 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Mon Jun 02 15:36:08 PDT 2025
;; MSG SIZE  rcvd: 45


┌──(kali㉿kali)-[~]
└─$ dig example.com @8.8.8.8

; <<>> DiG 9.20.9-1-Debian <<>> example.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7986
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            0       IN      A       23.215.0.136

;; Query time: 56 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Jun 02 15:38:46 PDT 2025
;; MSG SIZE  rcvd: 45


┌──(kali㉿kali)-[~]
└─$ 
```