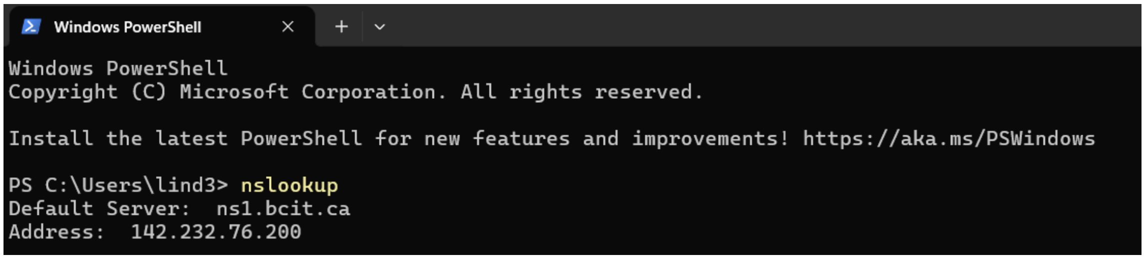
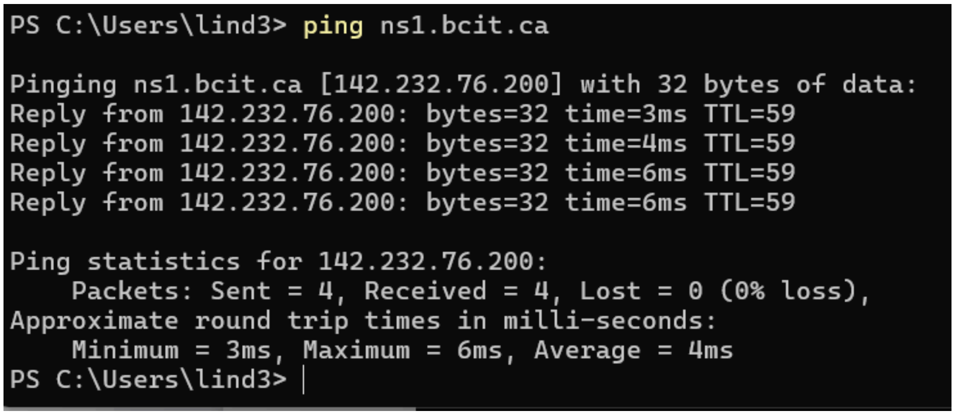
Lindy Cagalawan
A00850095

ACIT 1620 Lab — DNS with nslookup, dig and Wireshark

2.1 Identify your default DNS resolver



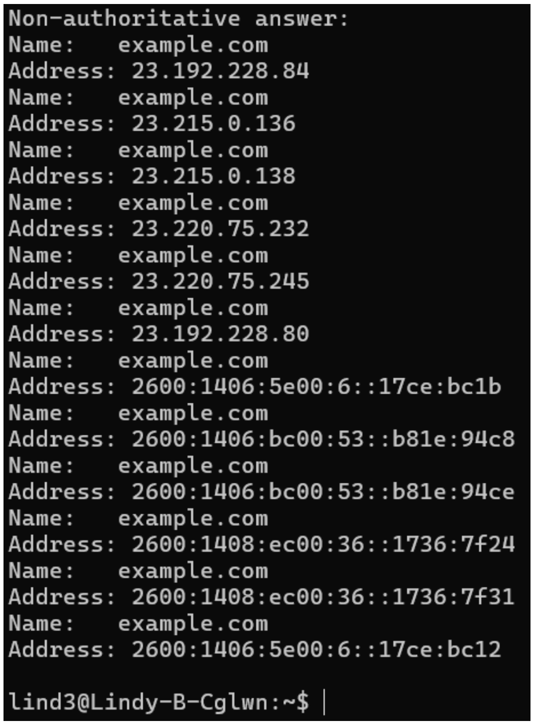
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\lind3> nslookup
Default Server:  ns1.bcit.ca
Address:  142.232.76.200
```



```
PS C:\Users\lind3> ping ns1.bcit.ca

Pinging ns1.bcit.ca [142.232.76.200] with 32 bytes of data:
Reply from 142.232.76.200: bytes=32 time=3ms TTL=59
Reply from 142.232.76.200: bytes=32 time=4ms TTL=59
Reply from 142.232.76.200: bytes=32 time=6ms TTL=59
Reply from 142.232.76.200: bytes=32 time=6ms TTL=59

Ping statistics for 142.232.76.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
PS C:\Users\lind3>
```

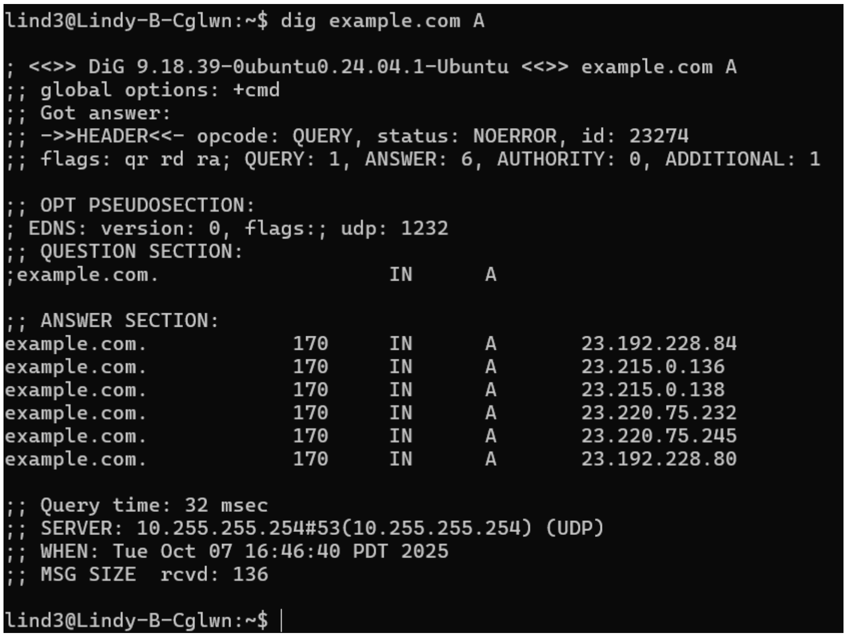
Resolver IP: 142.232.76.200

3.1 — nslookup example.com



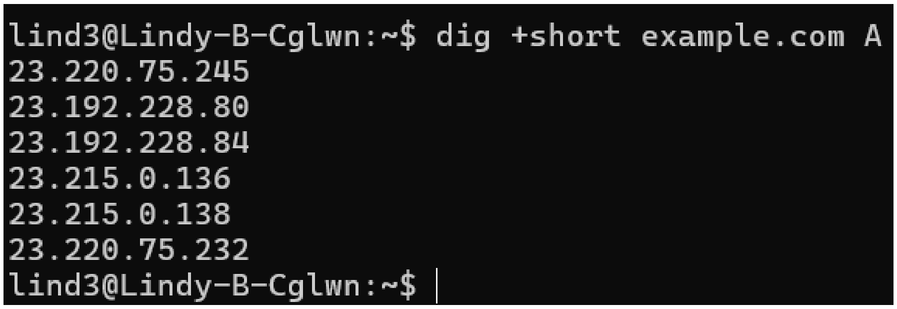
```
Non-authoritative answer:
Name:    example.com
Address: 23.192.228.84
Name:    example.com
Address: 23.215.0.136
Name:    example.com
Address: 23.215.0.138
Name:    example.com
Address: 23.220.75.232
Name:    example.com
Address: 23.220.75.245
Name:    example.com
Address: 23.192.228.80
Name:    example.com
Address: 2600:1406:5e00:6::17ce:bc1b
Name:    example.com
Address: 2600:1406:bc00:53::b81e:94c8
Name:    example.com
Address: 2600:1406:bc00:53::b81e:94ce
Name:    example.com
Address: 2600:1408:ec00:36::1736:7f24
Name:    example.com
Address: 2600:1408:ec00:36::1736:7f31
Name:    example.com
Address: 2600:1406:5e00:6::17ce:bc12

lind3@Lindy-B-Cglwn:~$
```

Step 3.2 — dig example.com A



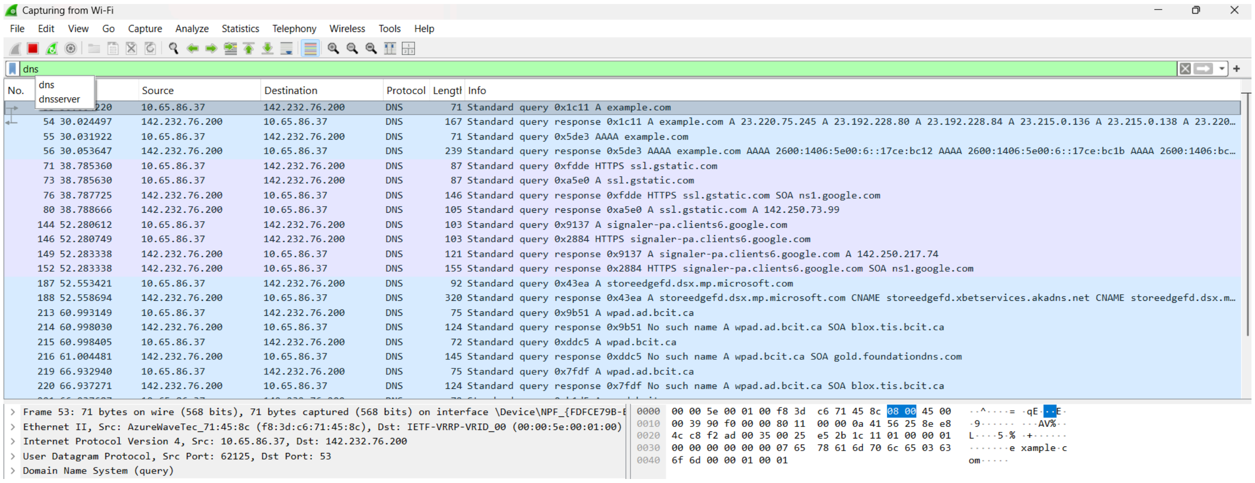
```
lind3@Lindy-B-Cglwn:~$ dig example.com A

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> example.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23274
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            170     IN      A       23.192.228.84
example.com.            170     IN      A       23.215.0.136
example.com.            170     IN      A       23.215.0.138
example.com.            170     IN      A       23.220.75.232
example.com.            170     IN      A       23.220.75.245
example.com.            170     IN      A       23.192.228.80

;; Query time: 32 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Tue Oct 07 16:46:40 PDT 2025
;; MSG SIZE  rcvd: 136

lind3@Lindy-B-Cglwn:~$
```

Step 3.3 — Quick formats with dig +short



```
lind3@Lindy-B-Cglwn:~$ dig +short example.com A
23.220.75.245
23.192.228.80
23.192.228.84
23.215.0.136
23.215.0.138
23.220.75.232
lind3@Lindy-B-Cglwn:~$
```

Step 3.4 nslookup using Wireshark



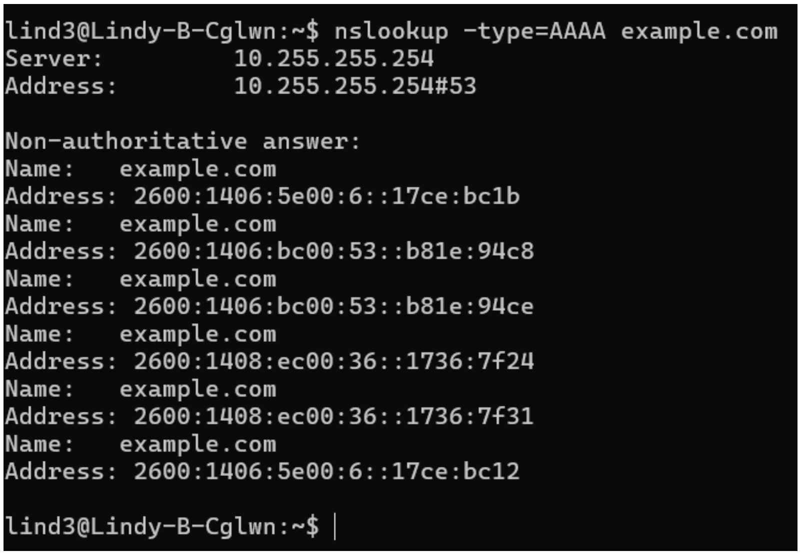
Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
	220	10.65.86.37	142.232.76.200	DNS	71	Standard query 0x1c11 A example.com
54	30.024497	142.232.76.200	10.65.86.37	DNS	167	Standard query response 0x1c11 A example.com A 23.220.75.245 A 23.192.228.80 A 23.192.228.84 A 23.215.0.136 A 23.215.0.138 A 23.220…
55	30.031922	10.65.86.37	142.232.76.200	DNS	71	Standard query 0x5de3 AAAA example.com
56	30.053647	142.232.76.200	10.65.86.37	DNS	239	Standard query response 0x5de3 AAAA example.com AAAA 2600:1406:5e00:6::17ce:bc12 AAAA 2600:1406:5e00:6::17ce:bc1b AAAA 2600:1406:bc…
71	38.785360	10.65.86.37	142.232.76.200	DNS	87	Standard query 0xfdde HTTPS ssl.gstatic.com
73	38.785630	10.65.86.37	142.232.76.200	DNS	87	Standard query 0xa5e0 A ssl.gstatic.com
76	38.787725	142.232.76.200	10.65.86.37	DNS	146	Standard query response 0xfdde HTTPS ssl.gstatic.com SOA ns1.google.com
80	38.788666	142.232.76.200	10.65.86.37	DNS	105	Standard query response 0xa5e0 A ssl.gstatic.com A 142.250.73.99
144	52.280612	10.65.86.37	142.232.76.200	DNS	103	Standard query 0x9137 A signaler-pa.clients6.google.com
146	52.280749	10.65.86.37	142.232.76.200	DNS	103	Standard query 0x2884 HTTPS signaler-pa.clients6.google.com
149	52.283338	142.232.76.200	10.65.86.37	DNS	121	Standard query response 0x9137 A signaler-pa.clients6.google.com A 142.250.217.74
152	52.283338	142.232.76.200	10.65.86.37	DNS	155	Standard query response 0x2884 HTTPS signaler-pa.clients6.google.com SOA ns1.google.com
187	52.553421	10.65.86.37	142.232.76.200	DNS	92	Standard query 0x43ea A storeedgefd.dsx.mp.microsoft.com
188	52.558694	142.232.76.200	10.65.86.37	DNS	320	Standard query response 0x43ea A storeedgefd.dsx.mp.microsoft.com CNAME storeedgefd.xbetservices.akadns.net CNAME storeedgefd.dsx.m…
213	60.993149	10.65.86.37	142.232.76.200	DNS	75	Standard query 0x9b51 A wpad.ad.bcit.ca
214	60.998030	142.232.76.200	10.65.86.37	DNS	124	Standard query response 0x9b51 No such name A wpad.ad.bcit.ca SOA blox.tis.bcit.ca
215	60.998405	10.65.86.37	142.232.76.200	DNS	72	Standard query 0xddc5 A wpad.bcit.ca
216	61.004481	142.232.76.200	10.65.86.37	DNS	145	Standard query response 0xddc5 No such name A wpad.bcit.ca SOA gold.foundationdns.com
219	66.932940	10.65.86.37	142.232.76.200	DNS	75	Standard query 0x7fdf A wpad.ad.bcit.ca
220	66.937271	142.232.76.200	10.65.86.37	DNS	124	Standard query response 0x7fdf No such name A wpad.ad.bcit.ca SOA blox.tis.bcit.ca

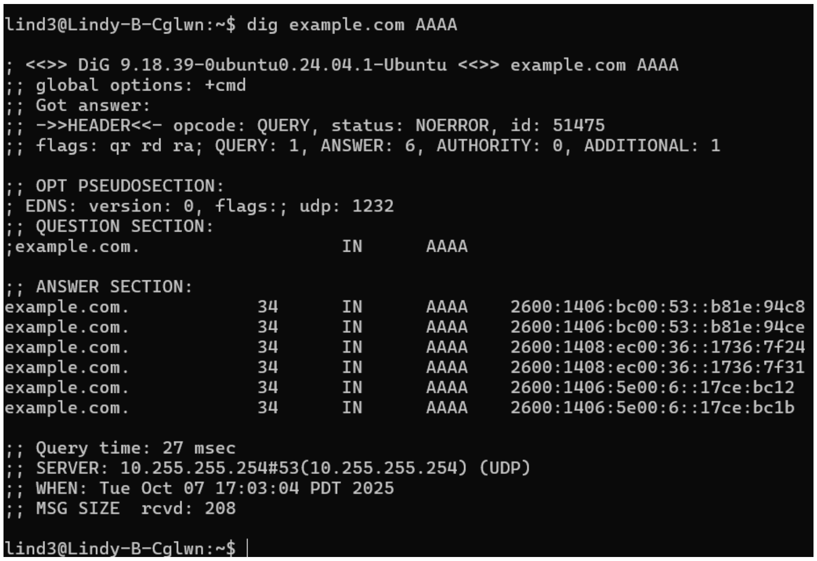
```
> Frame 53: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{FDFCE79B-E
> Ethernet II, Src: AzureWaveTec_71:45:8c (f8:3d:c6:71:45:8c), Dst: IETF-VRRP-VRID_00 (00:00:5e:00:01:00)
> Internet Protocol Version 4, Src: 10.65.86.37, Dst: 142.232.76.200
> User Datagram Protocol, Src Port: 62125, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 00 5e 00 01 00 f8 3d  c6 71 45 8c 08 00 45 00   ··^····= ·qE···E·
0010  00 39 90 f0 00 00 80 11  00 00 0a 41 56 25 8e e8   ·9······ ···AV%··
0020  4c c8 f2 ad 00 35 00 25  e5 2b 1c 11 01 00 00 01   L····5·% ·+······
0030  00 00 00 00 00 00 07 65  78 61 6d 70 6c 65 03 63   ·······e xample·c
0040  6f 6d 00 00 01 00 01                               om·····
```

Step 4.1 — IPv6 address (AAAA)

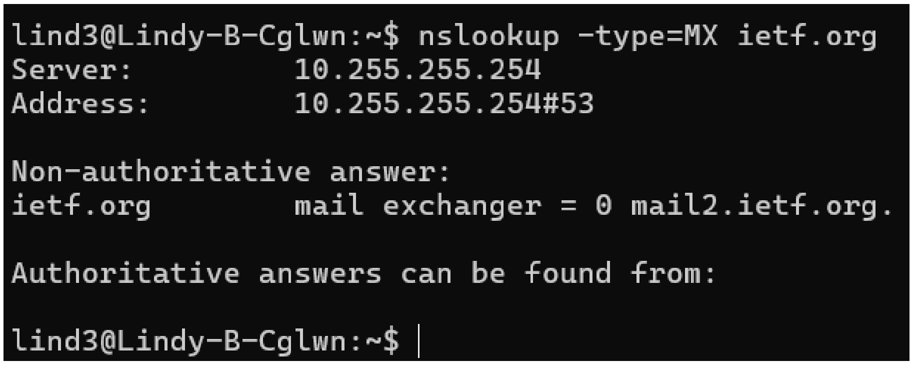


```
lind3@Lindy-B-Cglwn:~$ nslookup -type=AAAA example.com
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
Name:   example.com
Address: 2600:1406:5e00:6::17ce:bc1b
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94c8
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94ce
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f24
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f31
Name:   example.com
Address: 2600:1406:5e00:6::17ce:bc12

lind3@Lindy-B-Cglwn:~$
```

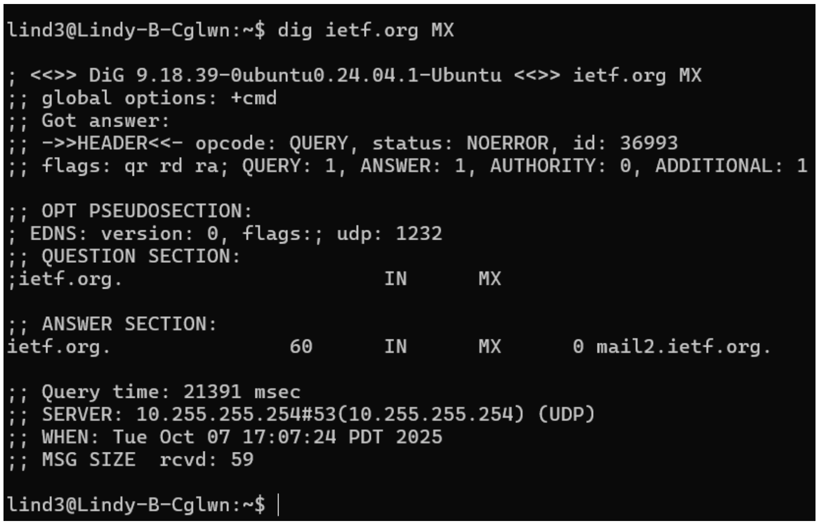


```
lind3@Lindy-B-Cglwn:~$ dig example.com AAAA

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> example.com AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51475
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;example.com.                   IN      AAAA

;; ANSWER SECTION:
example.com.            34      IN      AAAA    2600:1406:bc00:53::b81e:94c8
example.com.            34      IN      AAAA    2600:1406:bc00:53::b81e:94ce
example.com.            34      IN      AAAA    2600:1408:ec00:36::1736:7f24
example.com.            34      IN      AAAA    2600:1408:ec00:36::1736:7f31
example.com.            34      IN      AAAA    2600:1406:5e00:6::17ce:bc12
example.com.            34      IN      AAAA    2600:1406:5e00:6::17ce:bc1b

;; Query time: 27 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Tue Oct 07 17:03:04 PDT 2025
;; MSG SIZE  rcvd: 208

lind3@Lindy-B-Cglwn:~$
```

Step 4.2 — Mail exchangers (MX)

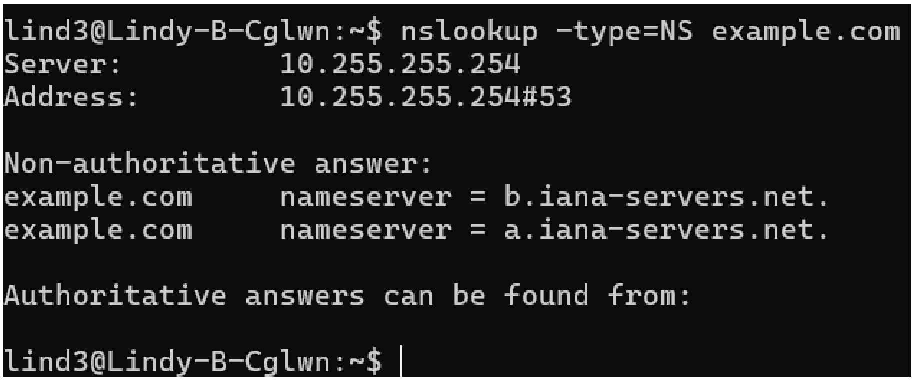


```
lind3@Lindy-B-Cglwn:~$ nslookup -type=MX ietf.org
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
ietf.org        mail exchanger = 0 mail2.ietf.org.

Authoritative answers can be found from:

lind3@Lindy-B-Cglwn:~$
```

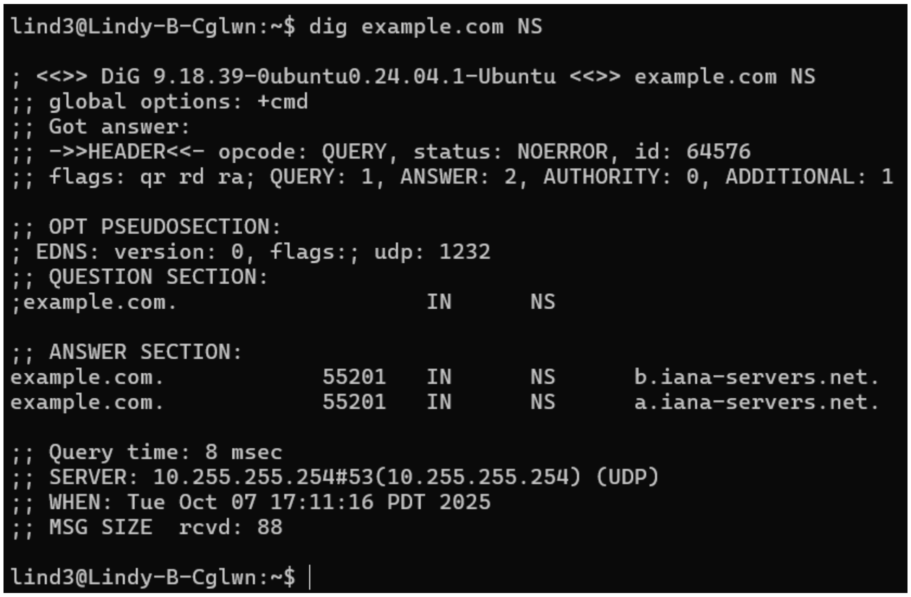


```
lind3@Lindy-B-Cglwn:~$ dig ietf.org MX

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> ietf.org MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36993
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ietf.org.                      IN      MX

;; ANSWER SECTION:
ietf.org.               60      IN      MX      0 mail2.ietf.org.

;; Query time: 21391 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Tue Oct 07 17:07:24 PDT 2025
;; MSG SIZE  rcvd: 59

lind3@Lindy-B-Cglwn:~$ |
```

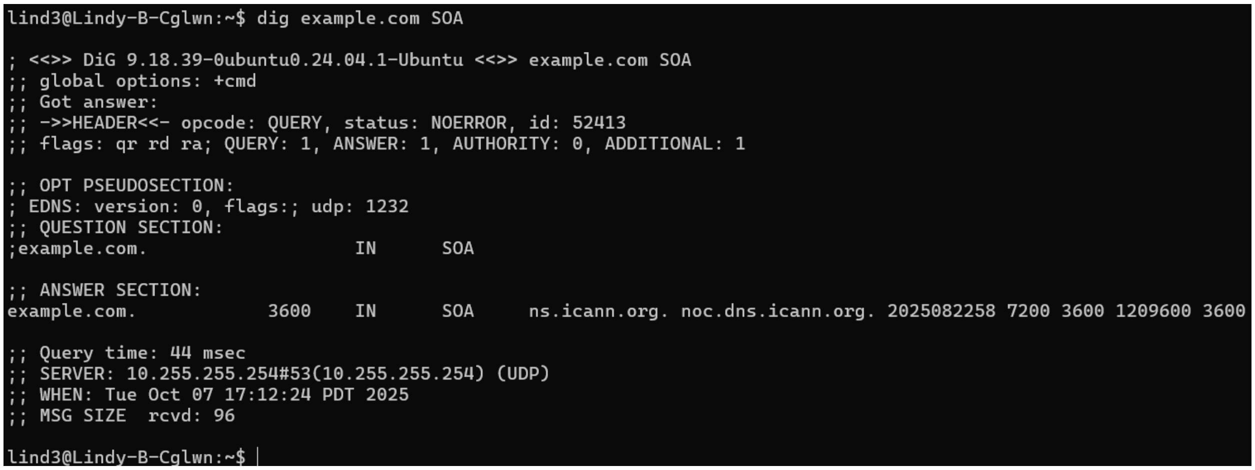
Step 4.3 — Name servers (NS) & Start of Authority (SOA)



```
lind3@Lindy-B-Cglwn:~$ nslookup -type=NS example.com
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
example.com     nameserver = b.iana-servers.net.
example.com     nameserver = a.iana-servers.net.

Authoritative answers can be found from:

lind3@Lindy-B-Cglwn:~$ |
```

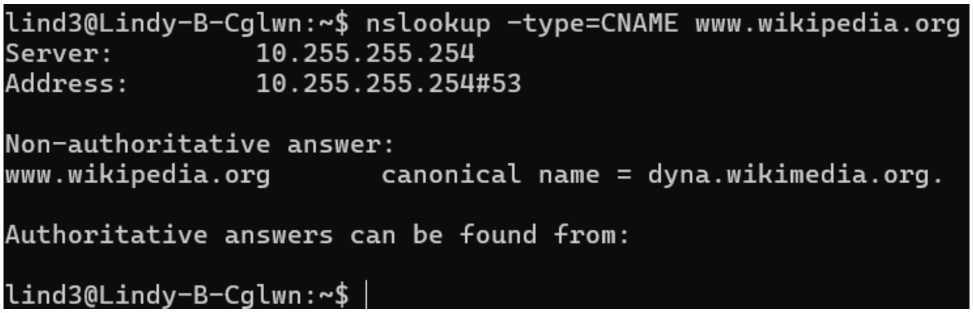


```
lind3@Lindy-B-Cglwn:~$ dig example.com NS

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> example.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64576
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;example.com.                   IN      NS

;; ANSWER SECTION:
example.com.            55201   IN      NS      b.iana-servers.net.
example.com.            55201   IN      NS      a.iana-servers.net.

;; Query time: 8 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Tue Oct 07 17:11:16 PDT 2025
;; MSG SIZE  rcvd: 88

lind3@Lindy-B-Cglwn:~$ |
```

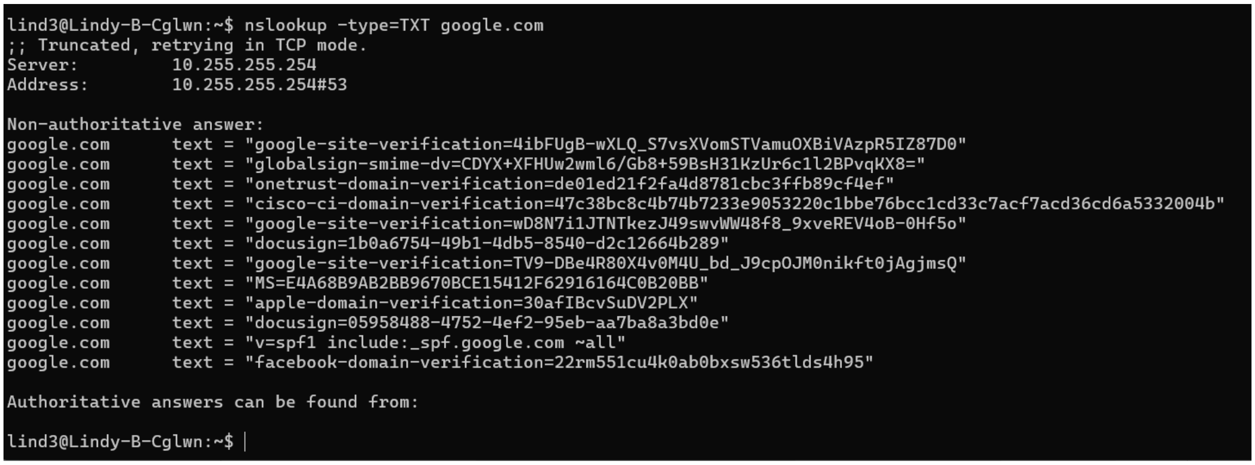


```
lind3@Lindy-B-Cglwn:~$ dig example.com SOA

; <<>> DiG 9.18.39-0ubuntu0.24.04.1-Ubuntu <<>> example.com SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52413
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;example.com.                   IN      SOA

;; ANSWER SECTION:
example.com.            3600    IN      SOA     ns.icann.org. noc.dns.icann.org. 2025082258 7200 3600 1209600 3600

;; Query time: 44 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Tue Oct 07 17:12:24 PDT 2025
;; MSG SIZE  rcvd: 96

lind3@Lindy-B-Cglwn:~$ 
```

Step 4.4 — Aliases (CNAME) & text records (TXT)



```
lind3@Lindy-B-Cglwn:~$ nslookup -type=CNAME www.wikipedia.org
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
www.wikipedia.org       canonical name = dyna.wikimedia.org.

Authoritative answers can be found from:

lind3@Lindy-B-Cglwn:~$ 
```



```
lind3@Lindy-B-Cglwn:~$ nslookup -type=TXT google.com
;; Truncated, retrying in TCP mode.
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
google.com      text = "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"
google.com      text = "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com      text = "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com      text = "cisco-ci-domain-verification=47c38bc8c4b74b7233e9053220c1bbe76bcc1cd33c7acf7acd36cd6a5332004b"
google.com      text = "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com      text = "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text = "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com      text = "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com      text = "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      text = "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com      text = "v=spf1 include:_spf.google.com ~all"
google.com      text = "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"

Authoritative answers can be found from:

lind3@Lindy-B-Cglwn:~$ 
```