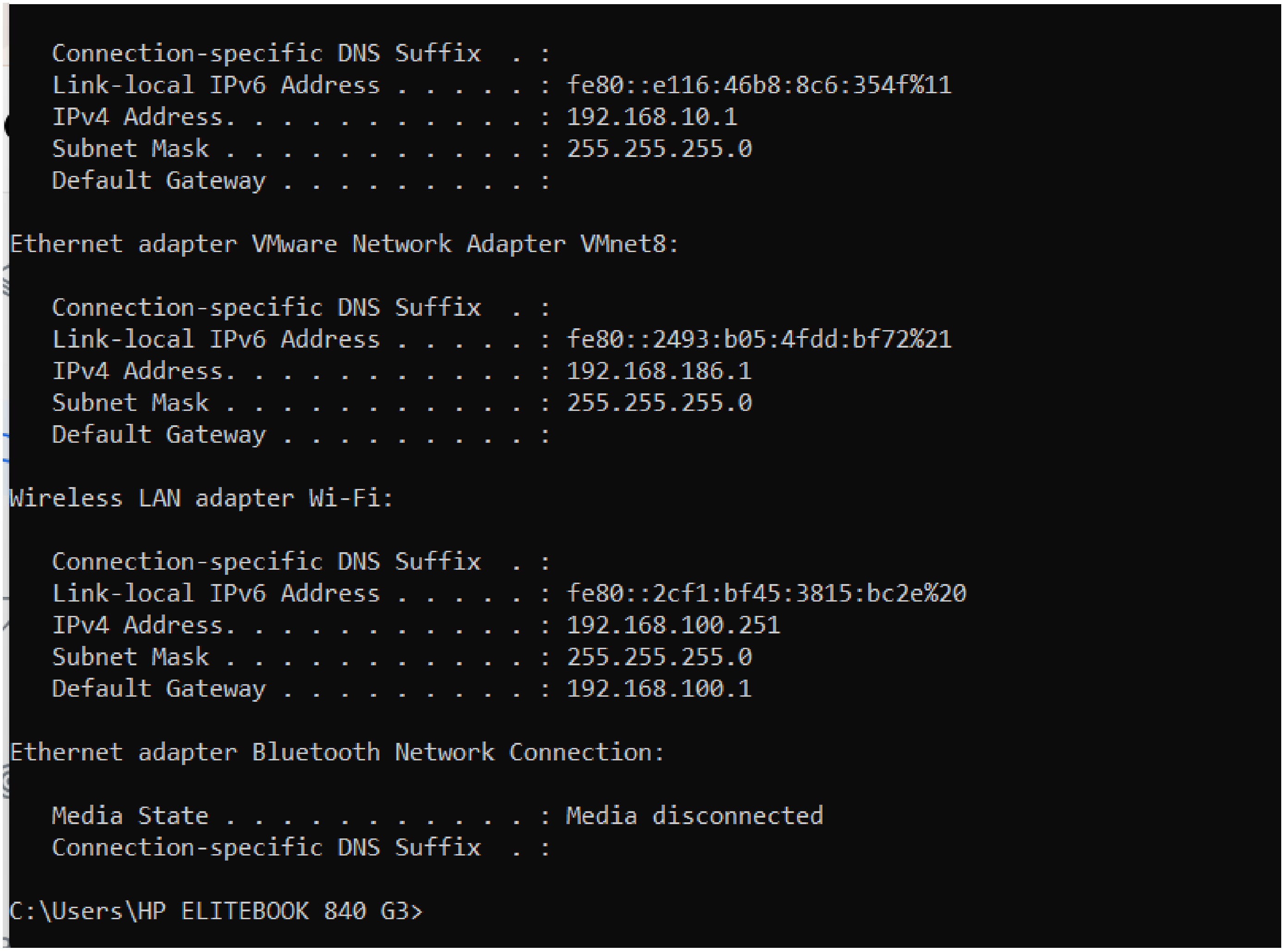
Check Point Networking 2.0

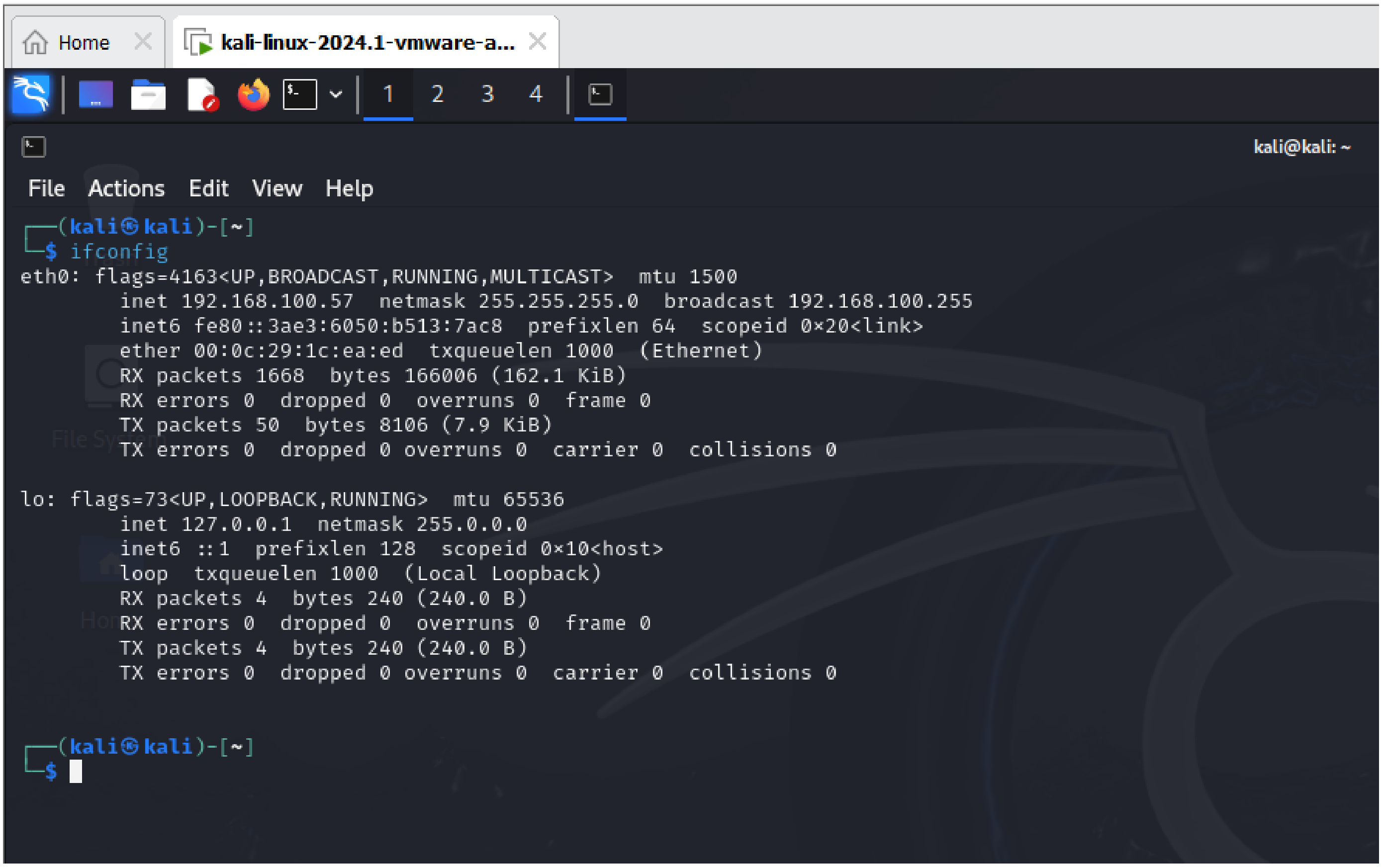
- First step you will use the following tools to identify the different IP address of the kali linux , windows and debian OS:

ipconfig



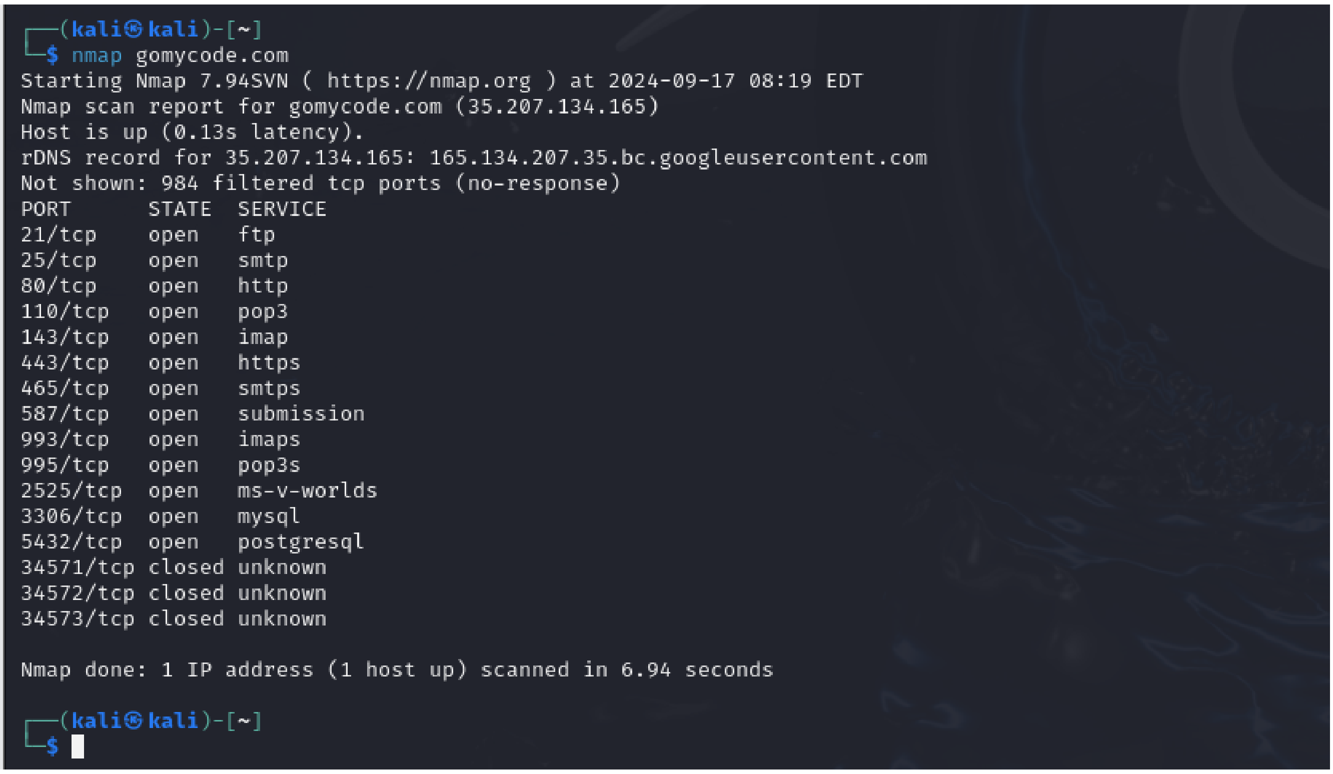
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e116:46b8:8c6:354f%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2493:b05:4fdd:bf72%21
   IPv4 Address. . . . . . . . . . . : 192.168.186.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2cf1:bf45:3815:bc2e%20
   IPv4 Address. . . . . . . . . . . : 192.168.100.251
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\HP ELITEBOOK 840 G3>
```

ifconfig



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.57  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::3ae3:6050:b513:7ac8  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:1c:ea:ed  txqueuelen 1000  (Ethernet)
        RX packets 1668  bytes 166006 (162.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50  bytes 8106 (7.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

- Using nmap identify the different ports running on The different machines

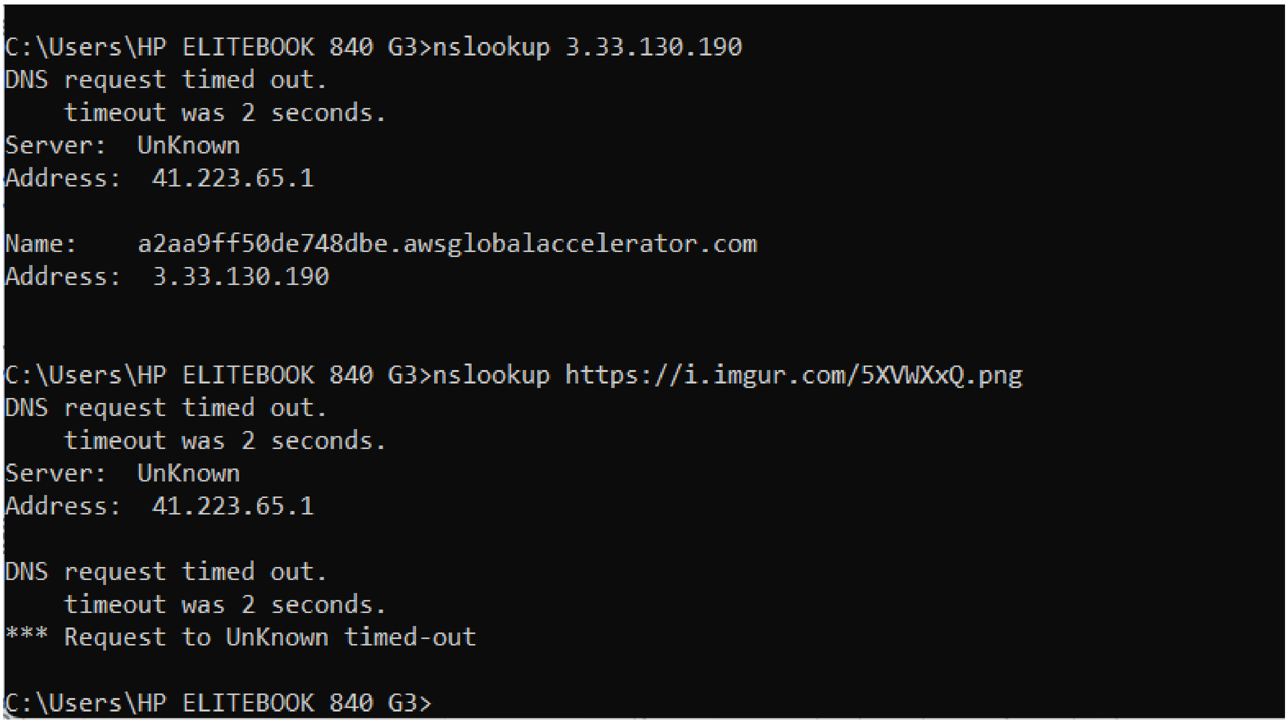


```
┌──(kali㉿kali)-[~]
└─$ nmap gomycode.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 08:19 EDT
Nmap scan report for gomycode.com (35.207.134.165)
Host is up (0.13s latency).
rDNS record for 35.207.134.165: 165.134.207.35.bc.googleusercontent.com
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    open   smtp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
2525/tcp  open   ms-v-worlds
3306/tcp  open   mysql
5432/tcp  open   postgresql
34571/tcp closed unknown
34572/tcp closed unknown
34573/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

  - using nslookup try to identify the FQND of the following IP : 3.33.130.190

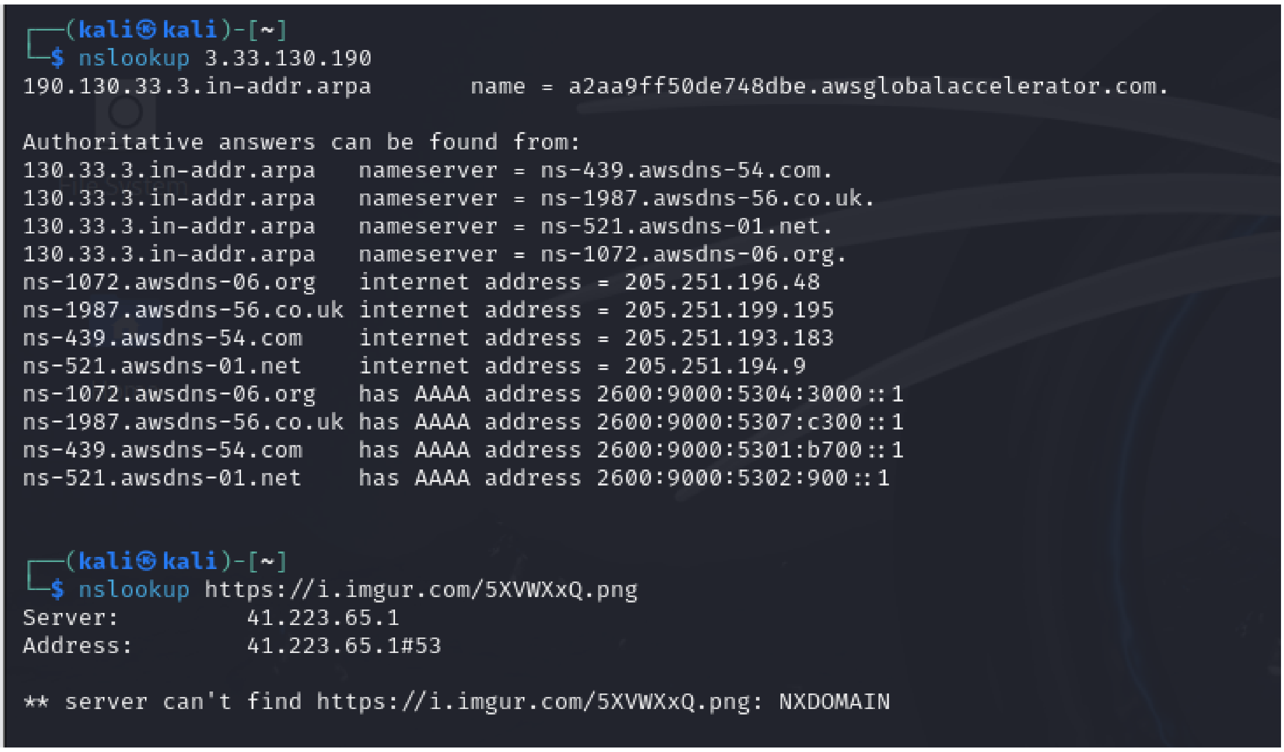
    https://i.imgur.com/5XVWXxQ.png

    WINDOWS OUTPUT



```
C:\Users\HP ELITEBOOK 840 G3>nslookup 3.33.130.190
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  41.223.65.1

Name:    a2aa9ff50de748dbe.awsglobalaccelerator.com
Address:  3.33.130.190


C:\Users\HP ELITEBOOK 840 G3>nslookup https://i.imgur.com/5XVWXxQ.png
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  41.223.65.1

DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\HP ELITEBOOK 840 G3>
```

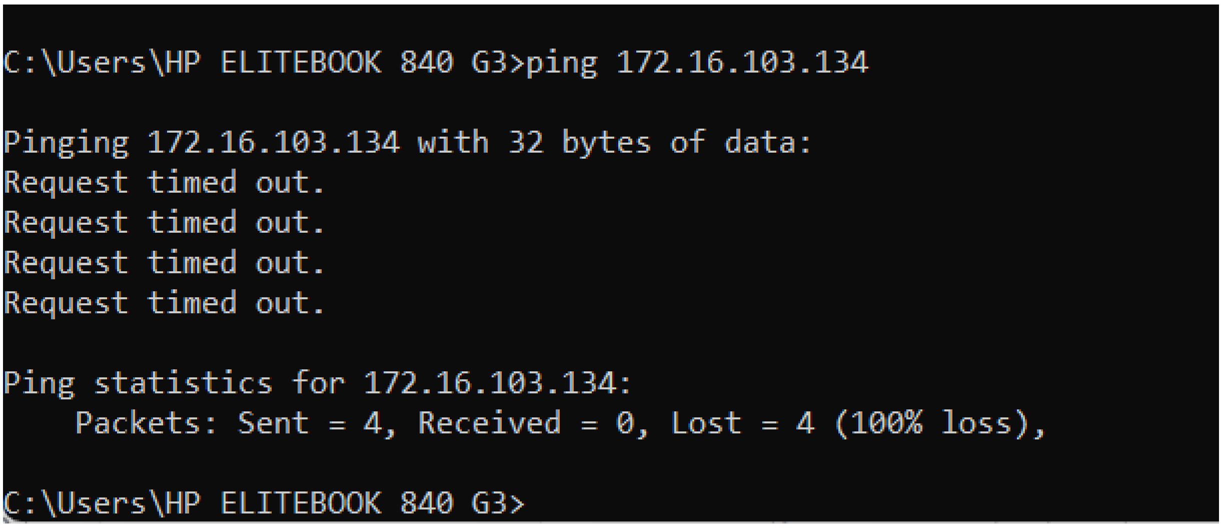
- **LINUX OUTPUT**



```
┌──(kali㉿kali)-[~]
└─$ nslookup 3.33.130.190
190.130.33.3.in-addr.arpa       name = a2aa9ff50de748dbe.awsglobalaccelerator.com.

Authoritative answers can be found from:
130.33.3.in-addr.arpa   nameserver = ns-439.awsdns-54.com.
130.33.3.in-addr.arpa   nameserver = ns-1987.awsdns-56.co.uk.
130.33.3.in-addr.arpa   nameserver = ns-521.awsdns-01.net.
130.33.3.in-addr.arpa   nameserver = ns-1072.awsdns-06.org.
ns-1072.awsdns-06.org   internet address = 205.251.196.48
ns-1987.awsdns-56.co.uk internet address = 205.251.199.195
ns-439.awsdns-54.com    internet address = 205.251.193.183
ns-521.awsdns-01.net    internet address = 205.251.194.9
ns-1072.awsdns-06.org   has AAAA address 2600:9000:5304:3000::1
ns-1987.awsdns-56.co.uk has AAAA address 2600:9000:5307:c300::1
ns-439.awsdns-54.com    has AAAA address 2600:9000:5301:b700::1
ns-521.awsdns-01.net    has AAAA address 2600:9000:5302:900::1


┌──(kali㉿kali)-[~]
└─$ nslookup https://i.imgur.com/5XVWXxQ.png
Server:         41.223.65.1
Address:        41.223.65.1#53

** server can't find https://i.imgur.com/5XVWXxQ.png: NXDOMAIN
```

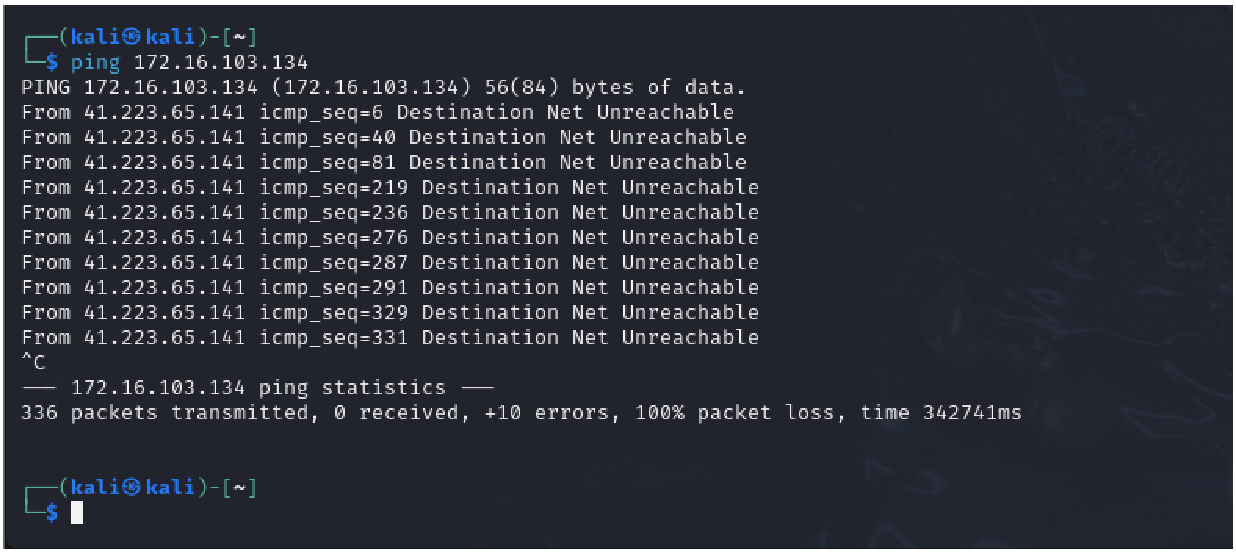
  - verify the communication with the following ip : 172.16.103.134 (use ping)

    WINDOWS OUTPUT



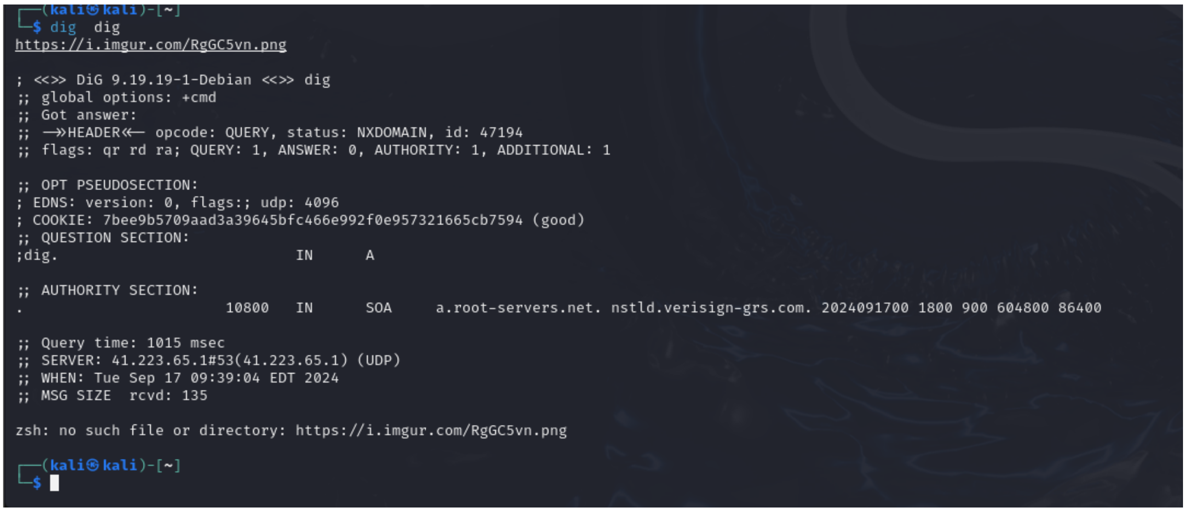
```
C:\Users\HP ELITEBOOK 840 G3>ping 172.16.103.134

Pinging 172.16.103.134 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.103.134:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\HP ELITEBOOK 840 G3>
```

LINUX OUTPUT



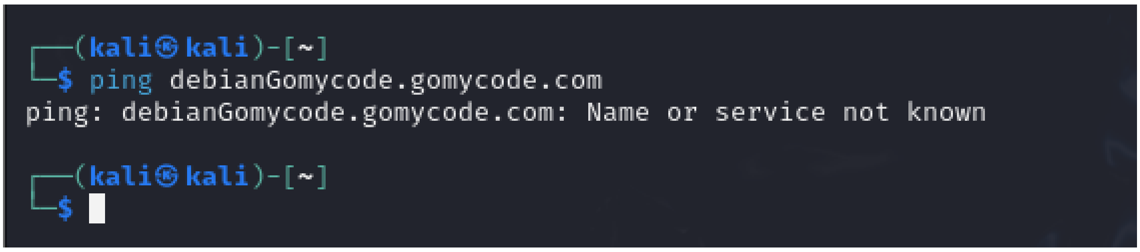
```
┌──(kali㉿kali)-[~]
└─$ ping 172.16.103.134
PING 172.16.103.134 (172.16.103.134) 56(84) bytes of data.
From 41.223.65.141 icmp_seq=6 Destination Net Unreachable
From 41.223.65.141 icmp_seq=40 Destination Net Unreachable
From 41.223.65.141 icmp_seq=81 Destination Net Unreachable
From 41.223.65.141 icmp_seq=219 Destination Net Unreachable
From 41.223.65.141 icmp_seq=236 Destination Net Unreachable
From 41.223.65.141 icmp_seq=276 Destination Net Unreachable
From 41.223.65.141 icmp_seq=287 Destination Net Unreachable
From 41.223.65.141 icmp_seq=291 Destination Net Unreachable
From 41.223.65.141 icmp_seq=329 Destination Net Unreachable
From 41.223.65.141 icmp_seq=331 Destination Net Unreachable
^C
── 172.16.103.134 ping statistics ──
336 packets transmitted, 0 received, +10 errors, 100% packet loss, time 342741ms


┌──(kali㉿kali)-[~]
└─$ █
```

- let’s try to identify it’s FQND : use dig
  https://i.imgur.com/RgGC5vn.png

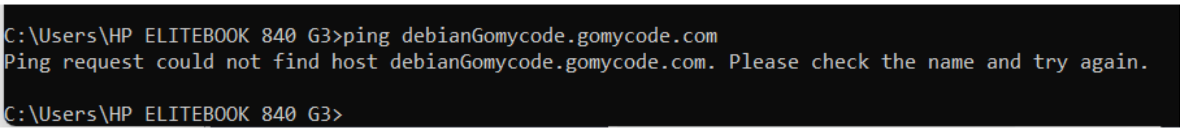


```
┌──(kali㉿kali)-[~]
└─$ dig  dig
https://i.imgur.com/RgGC5vn.png

; <<>> DiG 9.19.19-1-Debian <<>> dig
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47194
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7bee9b5709aad3a39645bfc466e992f0e957321665cb7594 (good)
;; QUESTION SECTION:
;dig.                           IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024091700 1800 900 604800 86400

;; Query time: 1015 msec
;; SERVER: 41.223.65.1#53(41.223.65.1) (UDP)
;; WHEN: Tue Sep 17 09:39:04 EDT 2024
;; MSG SIZE  rcvd: 135

zsh: no such file or directory: https://i.imgur.com/RgGC5vn.png

┌──(kali㉿kali)-[~]
└─$ █
```

- let’s re-verify by pinging : debianGomycode.gomycode.com



```
┌──(kali㉿kali)-[~]
└─$ ping debianGomycode.gomycode.com
ping: debianGomycode.gomycode.com: Name or service not known

┌──(kali㉿kali)-[~]
└─$ 
```

- 

```
C:\Users\HP ELITEBOOK 840 G3>ping debianGomycode.gomycode.com
Ping request could not find host debianGomycode.gomycode.com. Please check the name and try again.

C:\Users\HP ELITEBOOK 840 G3>
```