LAB 17

Dig Command

Tool: Kali Linux

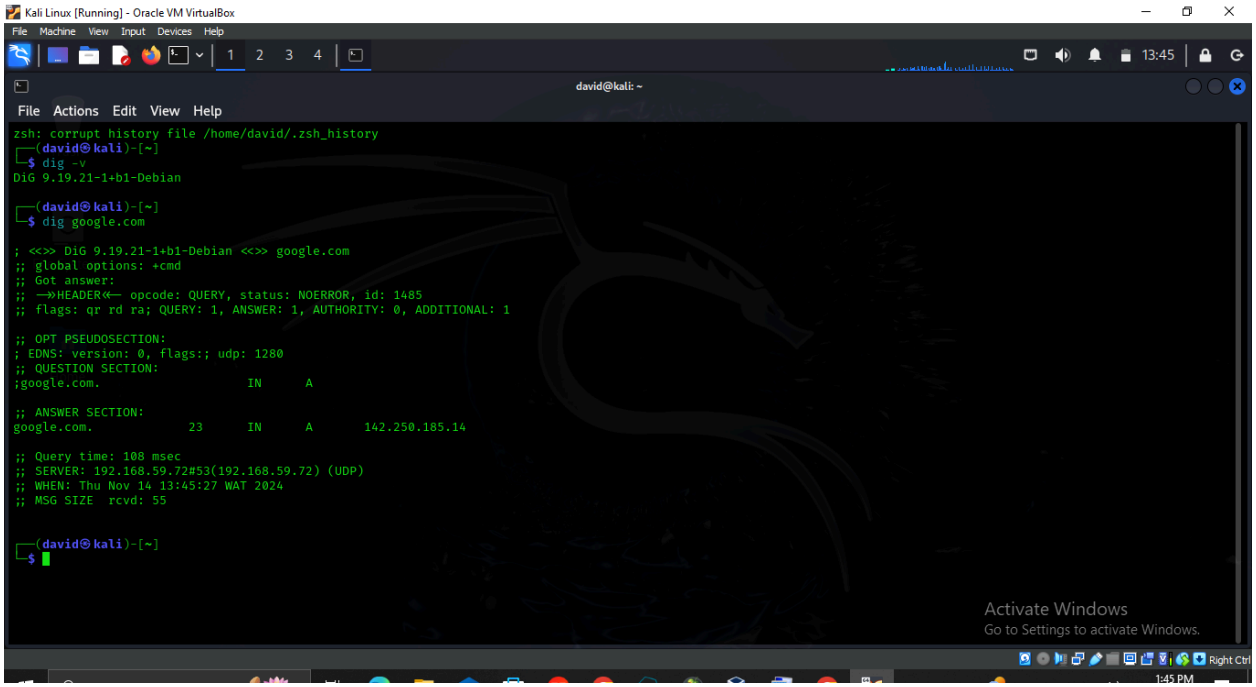
STEP 1: Dig is a tool which can be used on either Linux or Mac OS. Dig comes pre-installed on Kali Linux and you can check its version using the following command: dig -v

The dig syntax looks like the following:

Dig [server] [name] [type]

We will begin by performing a simple dig command. Type the following into a terminal:

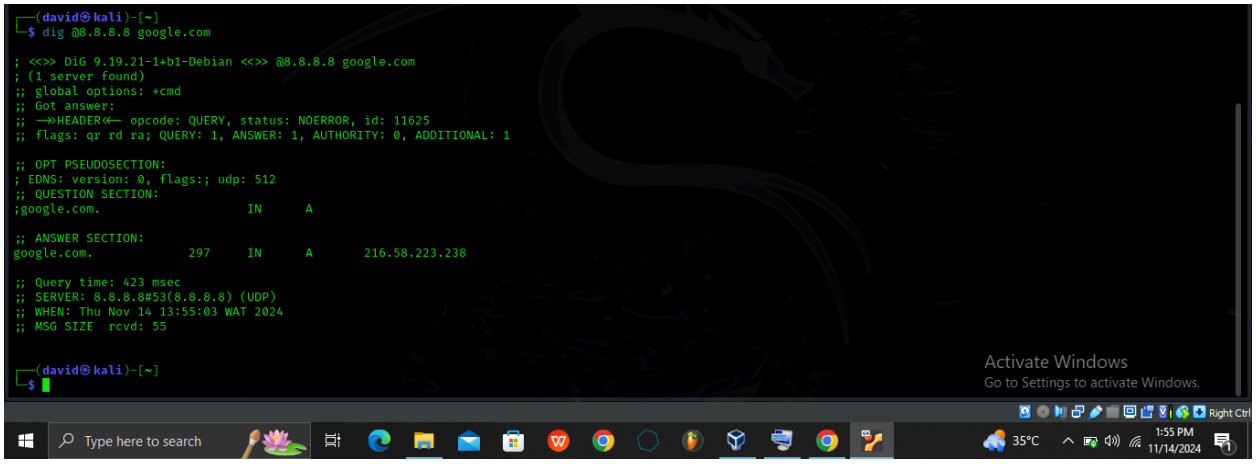
dig google.com



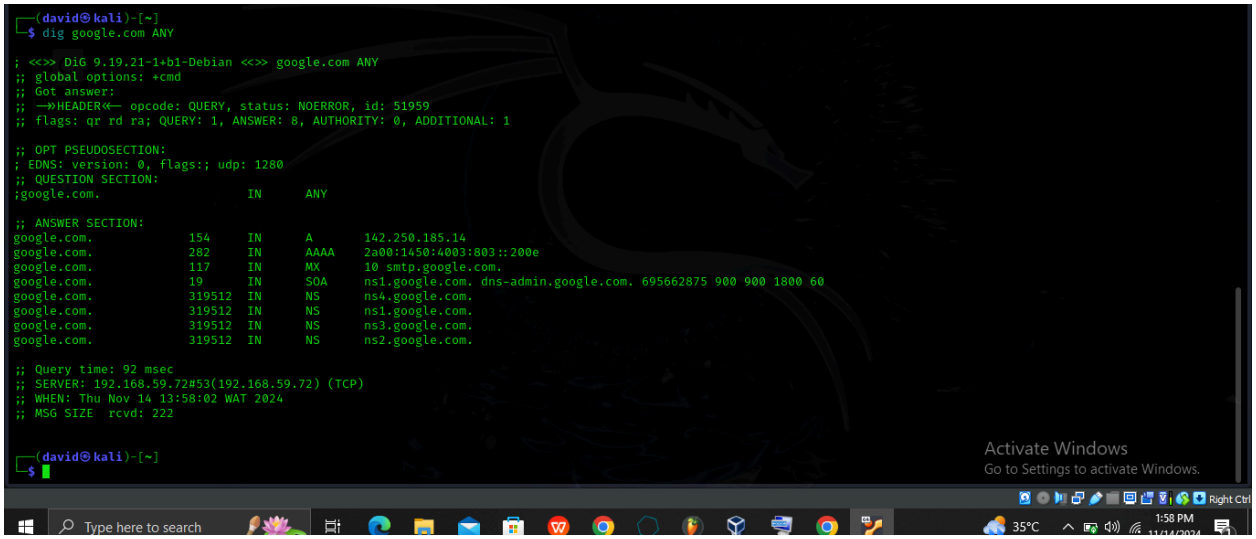
STEP 2: There may be a time when you only want the result of the query. This can be achieved in dig with the following command:
dig google.com +short

STEP 3:This next command will get rid of all information before the answer section, for easier reading. We can specify this using the following command:
dig google.com +noall +answer

STEP 4:We can also specify the nameservers we wish to query using the following command:
dig @8.8.8.8 google.com



STEP 5:If we want to query all DNS record types, we can use the “ANY” option. This will display all the available record types in the output:
dig google.com ANY

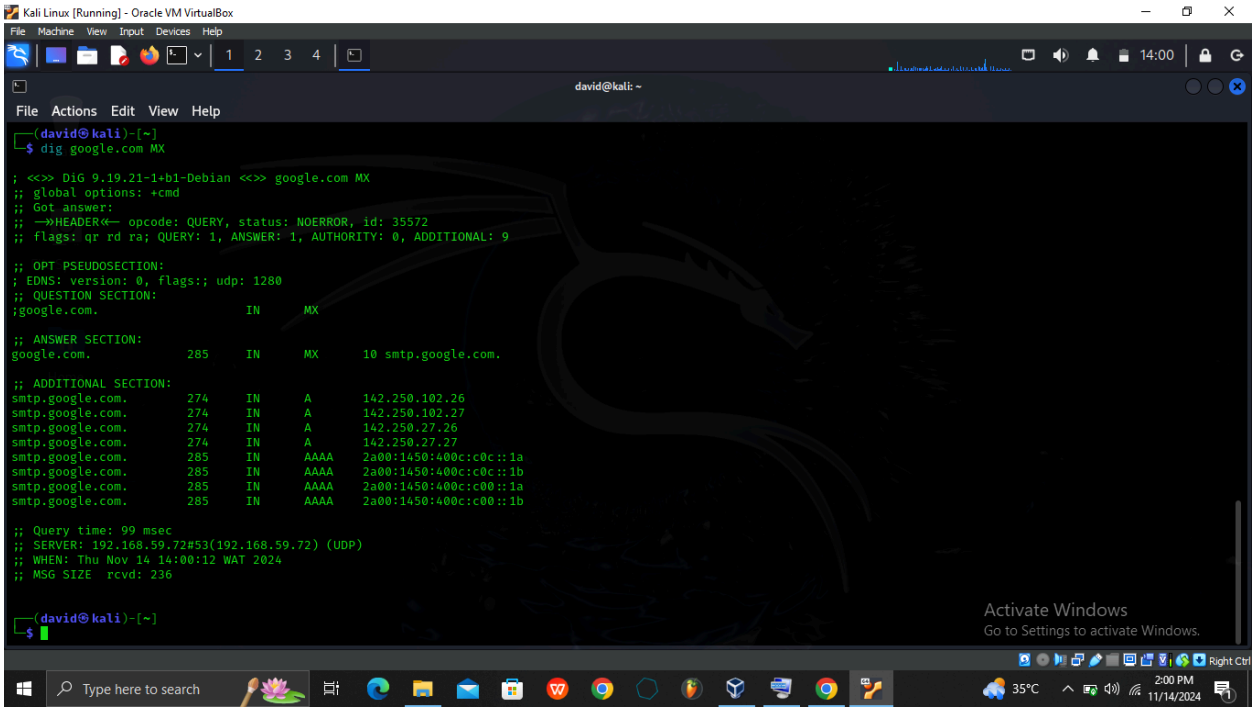


```
┌──(david㉿kali)-[~]
└─$ dig google.com ANY

; <<>> DiG 9.19.21-1+b1-Debian <<>> google.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51959
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             154     IN      A       142.250.185.14
google.com.             282     IN      AAAA    2a00:1450:4003:803::200e
google.com.             117     IN      MX      10 smtp.google.com.
google.com.             19      IN      SOA     ns1.google.com. dns-admin.google.com. 695662875 900 900 1800 60
google.com.             319512  IN      NS      ns4.google.com.
google.com.             319512  IN      NS      ns1.google.com.
google.com.             319512  IN      NS      ns3.google.com.
google.com.             319512  IN      NS      ns2.google.com.

;; Query time: 92 msec
;; SERVER: 192.168.59.72#53(192.168.59.72) (TCP)
;; WHEN: Thu Nov 14 13:58:02 WAT 2024
;; MSG SIZE  rcvd: 222


┌──(david㉿kali)-[~]
└─$
```

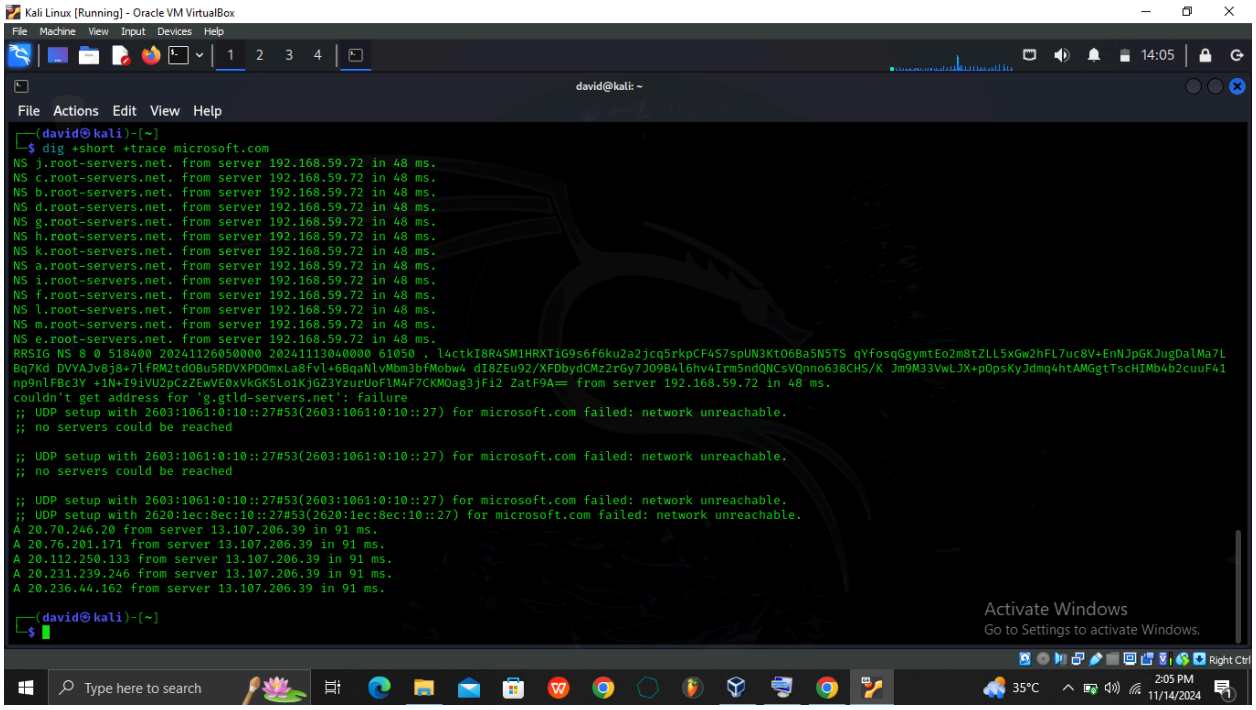
STEP 6: We can also look up a specific record. For example, if we want to get only the mail exchange section associated with a domain, we can use the following command: dig google.com MX

We can query a number of specific record types using the following tags in place of MX:

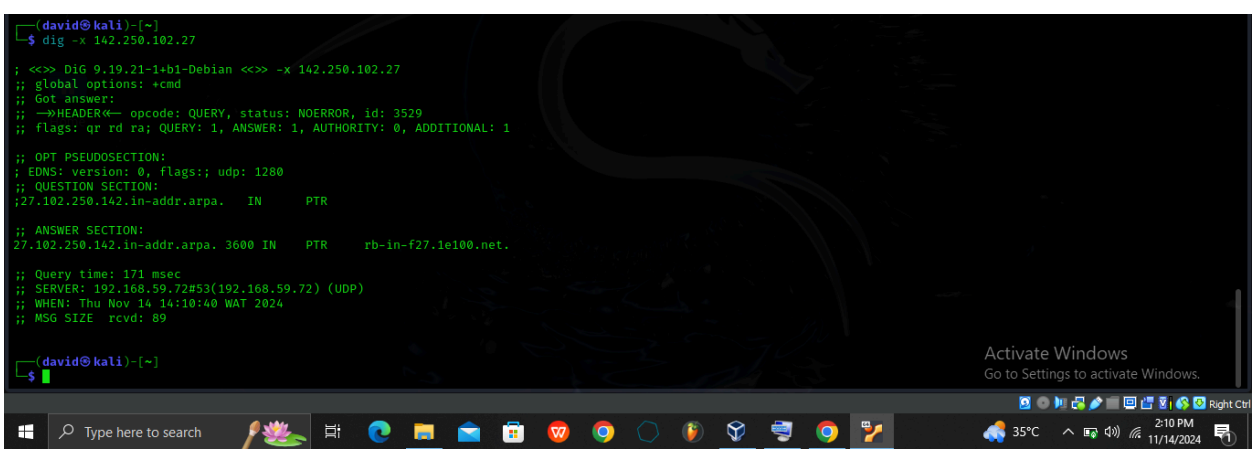
TXT, CNAME, NS, A



STEP 7:We can trace the DNS path with traceroute, using the following command:
dig +short +trace microsoft.com



STEP 8: We can trace the DNS path, similar to traceroute, using the following command:
dig -x 142.250.102.27



STEP 9: It is possible to access domain verification data by making a DNS TXT query. Dig is a tool with multiple uses and can be very useful for gathering a broad range of DNS information about a target site.

dig +short TXT hackaday.com