

## LAB 17

### Dig Command

Tool: Kali Linux

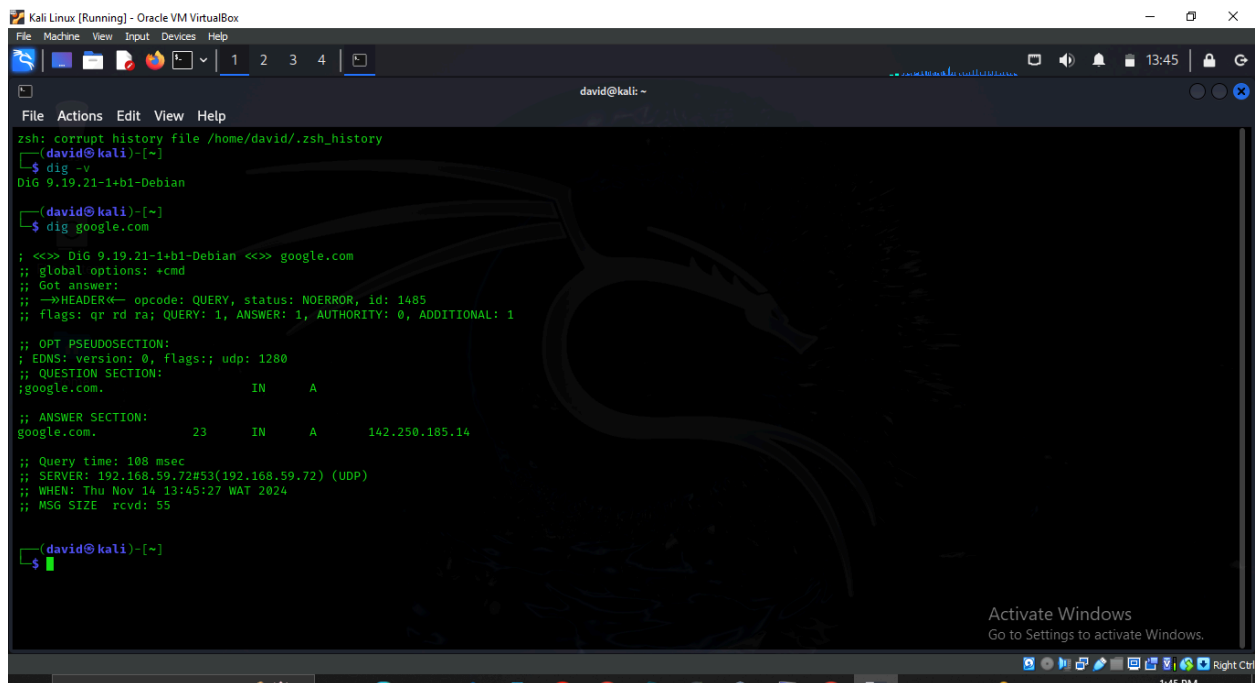
STEP 1: Dig is a tool which can be used on either Linux or Mac OS. Dig comes pre-installed on Kali Linux and you can check its version using the following command:  
`dig -v`

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`



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
david@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/david/.zsh_history
(david@kali)~$ dig -v
Dig 9.19.21-1+b1-Debian
(david@kali)~$ dig google.com
;; <<>> Dig 9.19.21-1+b1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 1485
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                IN      A
;; ANSWER SECTION:
google.com.                23      IN      A      142.250.185.14
;; Query time: 108 msec
;; SERVER: 192.168.59.72#53(192.168.59.72) (UDP)
;; WHEN: Thu Nov 14 13:45:27 WAT 2024
;; MSG SIZE rcvd: 55
(david@kali)~$
```

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

```
(david@kali)-[~]
$ dig google.com +short
142.250.185.14

(david@kali)-[~]
$
```



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

```
(david@kali)-[~]
$ dig google.com +noall +answer
google.com.      247    IN      A       142.250.185.14

(david@kali)-[~]
$
```



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

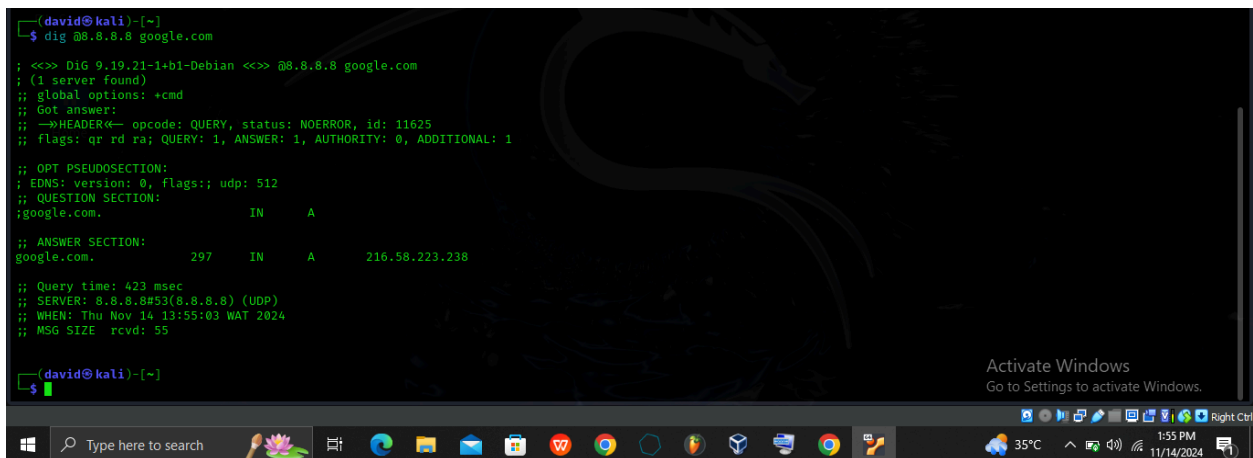
```
(david@kali)-[~]
$ dig @8.8.8.8 google.com

;<<>> Dig 9.19.21-1+b1-Debian <<>> @8.8.8.8 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 11625
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                IN      A
;; ANSWER SECTION:
google.com.                297    IN      A       216.58.223.238

;; Query time: 423 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Thu Nov 14 13:55:03 WAT 2024
;; MSG SIZE rcvd: 55

(david@kali)-[~]
$
```



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

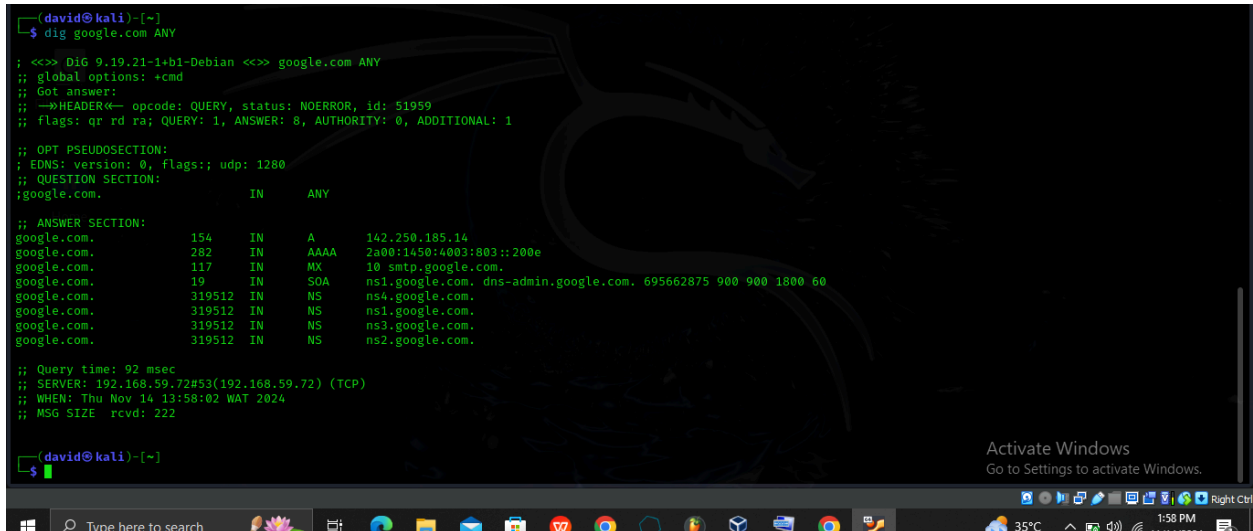
; <<>> DiG 9.19.21-1+b1-Debian <<>> google.com ANY
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 51959
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; 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

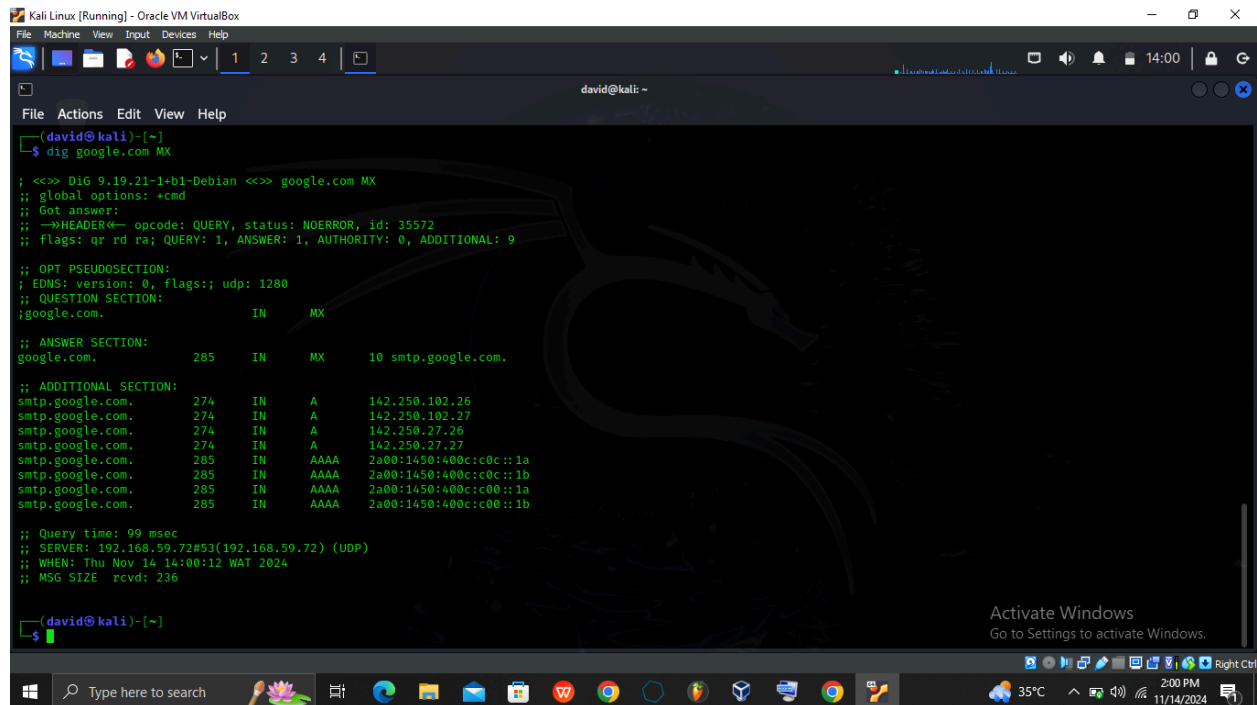
(david@kali)-[~]
```



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



```
(david@kali)-[~]
$ dig google.com MX

;<<> DiG 9.19.21-1+b1-Debian <<> google.com MX
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 35572
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 9

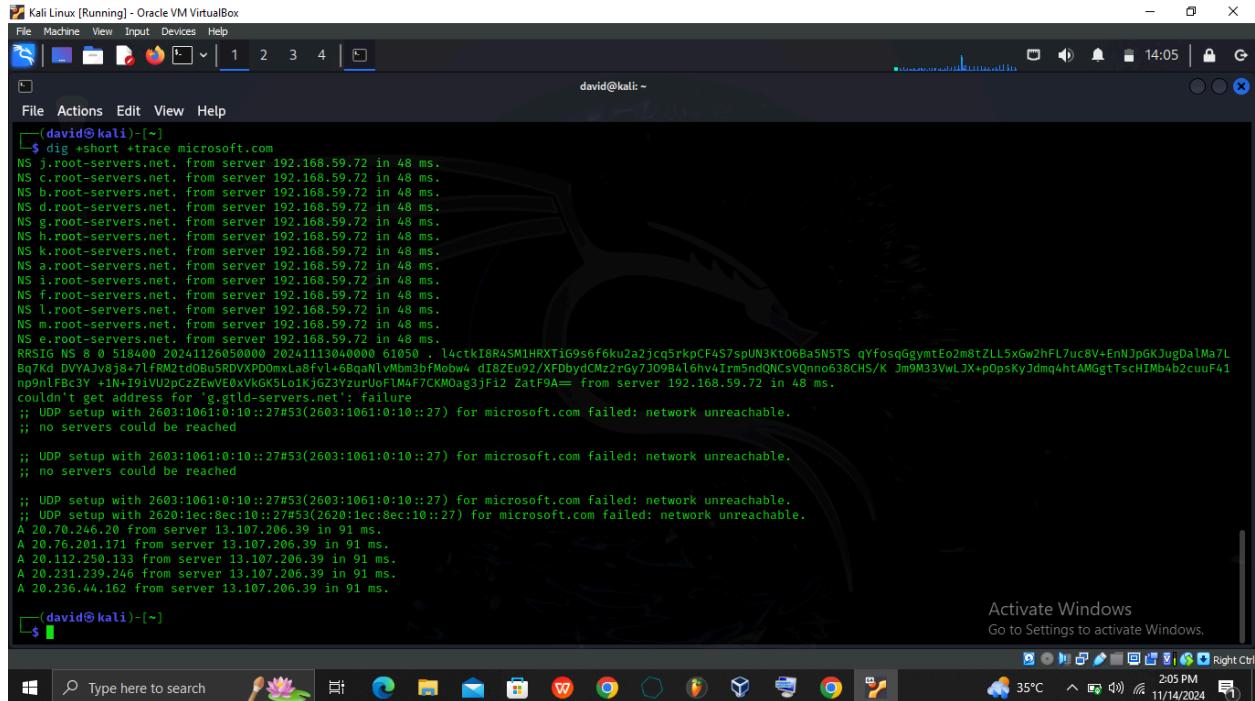
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                IN      MX
;; ANSWER SECTION:
google.com.                285     IN      MX      10 smtp.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.           274     IN      A        142.250.102.26
smtp.google.com.           274     IN      A        142.250.102.27
smtp.google.com.           274     IN      A        142.250.27.26
smtp.google.com.           274     IN      A        142.250.27.27
smtp.google.com.           285     IN      AAAA     2a00:1450:400c:c0c::1a
smtp.google.com.           285     IN      AAAA     2a00:1450:400c:c0c::1b
smtp.google.com.           285     IN      AAAA     2a00:1450:400c:c00::1a
smtp.google.com.           285     IN      AAAA     2a00:1450:400c:c00::1b

;; Query time: 99 msec
;; SERVER: 192.168.59.72#53(192.168.59.72) (UDP)
;; WHEN: Thu Nov 14 14:00:12 WAT 2024
;; MSG SIZE rcvd: 236

(david@kali)-[~]
$
```

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



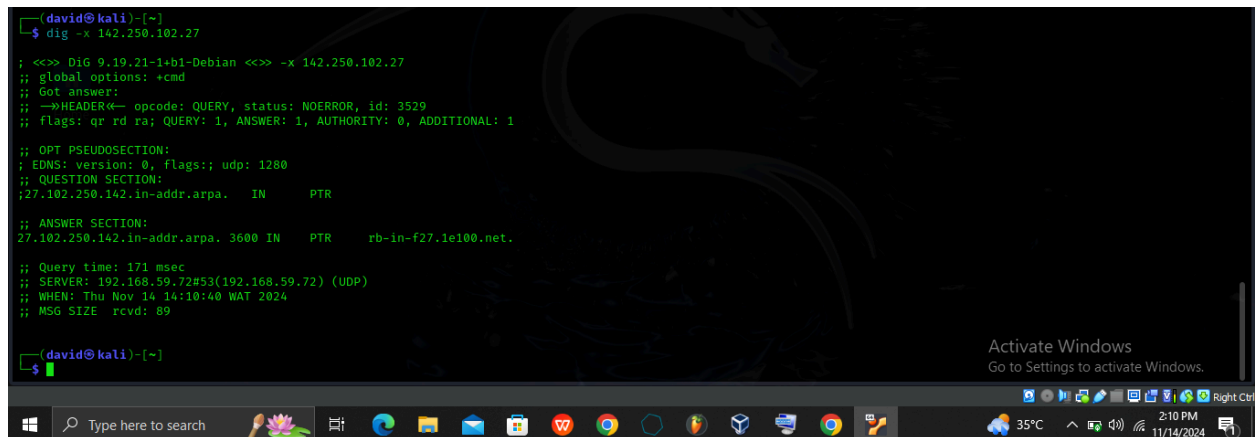
```
(david@kali)-[~]
$ dig +short +trace microsoft.com
NS j.root-servers.net. from server 192.168.59.72 in 48 ms.
NS c.root-servers.net. from server 192.168.59.72 in 48 ms.
NS b.root-servers.net. from server 192.168.59.72 in 48 ms.
NS d.root-servers.net. from server 192.168.59.72 in 48 ms.
NS g.root-servers.net. from server 192.168.59.72 in 48 ms.
NS h.root-servers.net. from server 192.168.59.72 in 48 ms.
NS k.root-servers.net. from server 192.168.59.72 in 48 ms.
NS a.root-servers.net. from server 192.168.59.72 in 48 ms.
NS i.root-servers.net. from server 192.168.59.72 in 48 ms.
NS f.root-servers.net. from server 192.168.59.72 in 48 ms.
NS l.root-servers.net. from server 192.168.59.72 in 48 ms.
NS m.root-servers.net. from server 192.168.59.72 in 48 ms.
NS e.root-servers.net. from server 192.168.59.72 in 48 ms.
RRSIG NS 8 0 518400 20241126050000 202411304000 61050 . l4ctk18R4SM1HRXT1G9s6f6ku2a2jcq5rpkCF4S7spUN3Kt06Ba5N5TS qYfosqGgymtEo2m8tZLL5xGw2hFL7uc8V+EnNJpGKJugDa1Ma7L
Bq7Kd DYYAJv818+7lFRM2td0BU5RDVXP0mXLa8fvl+6BqaNlVmbm3bfMobw4 dI8Zeu92/XFDbydCM2rGy7J09B4l6hv4Irm5ndQNCsVQnno638CHS/K Jm9M33VwLJX+pOpsKyJdmq4htAMGgtTschITMb4b2cuuF41
np9n1Fbc3Y +1N+191VU2pC2ZEWVe0xVKGK5Lo1KjGZ3YzUrUoFLM4F7CKMOag3jF12 ZatF9A= from server 192.168.59.72 in 48 ms.
;; couldn't get address for 'g.gtld-servers.net': failure
;; UDP setup with 2603:1061:0:10::27#53(2603:1061:0:10::27) for microsoft.com failed: network unreachable.
;; no servers could be reached

;; UDP setup with 2603:1061:0:10::27#53(2603:1061:0:10::27) for microsoft.com failed: network unreachable.
;; no servers could be reached

;; UDP setup with 2603:1061:0:10::27#53(2603:1061:0:10::27) for microsoft.com failed: network unreachable.
;; UDP setup with 2620:1ec:8ec:10::27#53(2620:1ec:8ec:10::27) for microsoft.com failed: network unreachable.
A 20.70.246.20 from server 13.107.206.39 in 91 ms.
A 20.76.201.171 from server 13.107.206.39 in 91 ms.
A 20.112.250.133 from server 13.107.206.39 in 91 ms.
A 20.231.239.246 from server 13.107.206.39 in 91 ms.
A 20.236.44.162 from server 13.107.206.39 in 91 ms.

(david@kali)-[~]
$
```

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



```
(david@kali)-[~]
$ dig -x 142.250.102.27
;<<>> DiG 9.19.21-1+b1-Debian <<>> -x 142.250.102.27
;; global options: +cmd
;; Got answer:
-->HEADER<-- opcode: QUERY, status: NOERROR, id: 3529
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

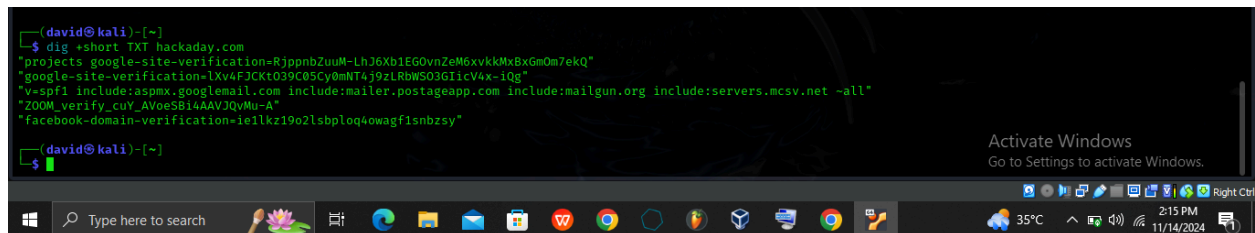
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1280
;; QUESTION SECTION:
; 27.102.250.142.in-addr.arpa. IN PTR
;; ANSWER SECTION:
27.102.250.142.in-addr.arpa. 3600 IN PTR rb-in-f27.1e100.net.

;; Query time: 171 msec
;; SERVER: 192.168.59.72#53(192.168.59.72) (UDP)
;; WHEN: Thu Nov 14 14:10:40 WAT 2024
;; MSG SIZE rcvd: 89

(david@kali)-[~]
$
```

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



```
(david@kali)-[~]
$ dig +short TXT hackaday.com
"projects google-site-verification-RjppnbZuuM-LhJ6Xb1EG0vnZeM6xykkMxBxGmQm7ekQ"
"google-site-verification-lXv4FJCKt039C85Cy0mNT4j9zLRbWS03GIcV4x-iQg"
"v=spf1 include:aspmx.googlemail.com include:mailer.postageapp.com include:mailgun.org include:servers.mcsv.net ~all"
"ZOOM_verify_cuY_AVoeSBi4AAVJQvMu-A"
"facebook-domain-verification=ie1lkz19o2lsbploq4owagf1snbzsy"

(david@kali)-[~]
$
```