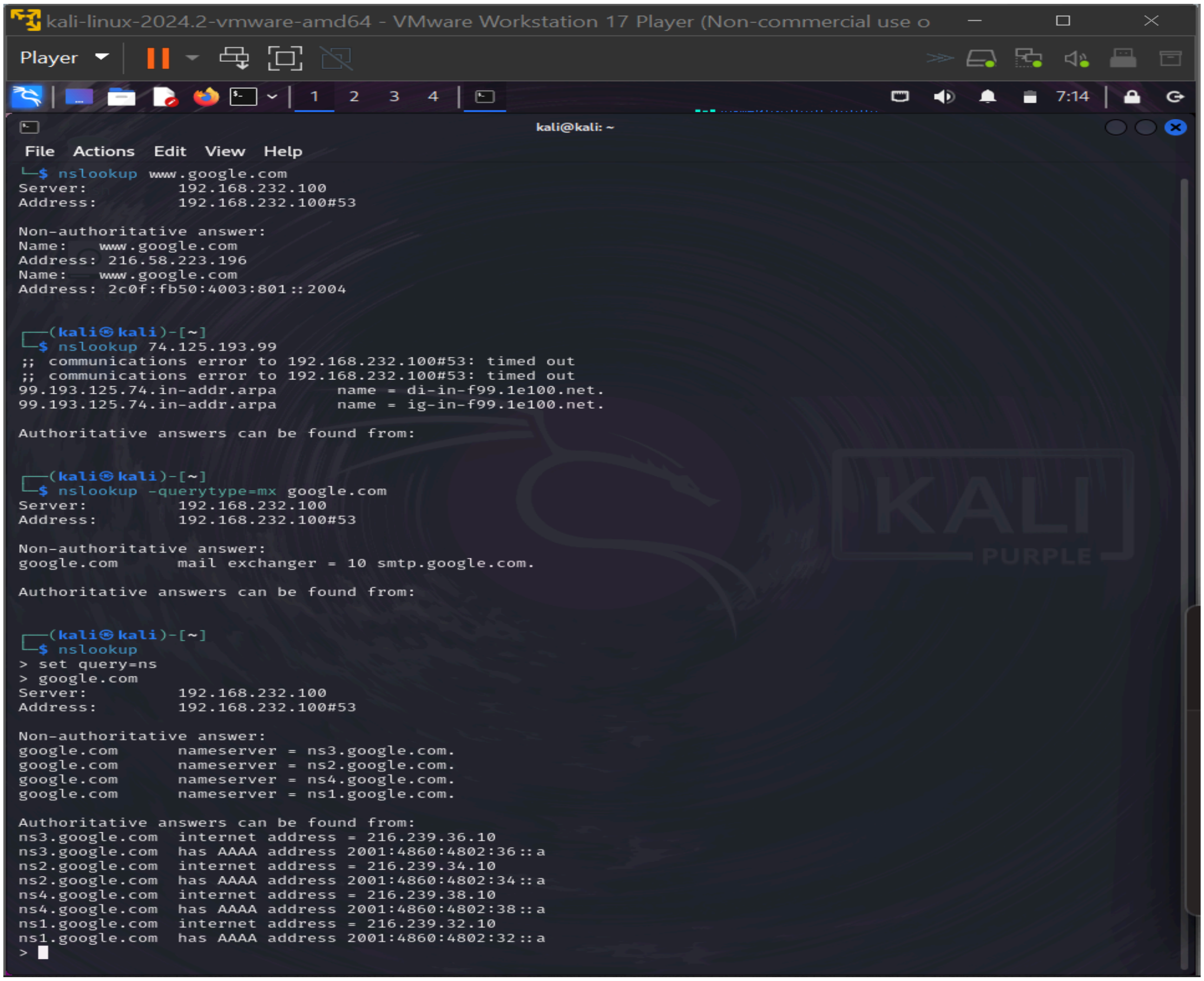
USAGE OF NSLOOKUP COMMAND

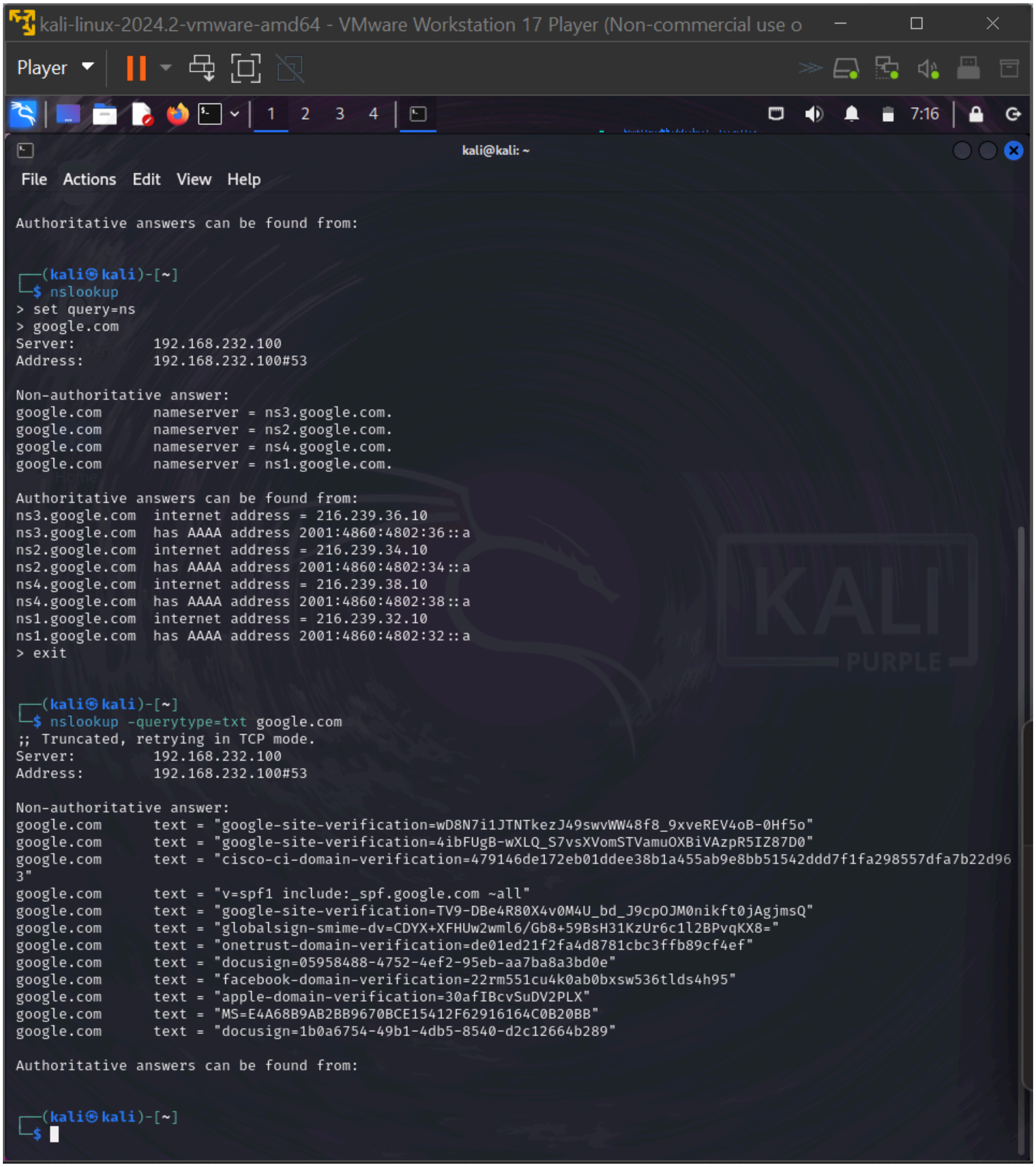
Tools : NSLOOKUP on Kali
Site : GOOGLE.COM

NSLOOKUP(short for **Name Server Lookup**) is a network utility used to query Domain Name System (DNS) servers to obtain information about domain names or IP addresses. It allows you to find details about domain names, such as the associated IP address, mail servers, and other DNS records.

INPUT FROM NSLOOKUP :


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use o
Player
1
2
3
4
7:14
kali@kali: ~
File
Actions
Edit
View
Help

```
└─$ nslookup www.google.com
Server:         192.168.232.100
Address:        192.168.232.100#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.223.196
Name:   www.google.com
Address: 2c0f:fb50:4003:801::2004


┌──(kali㉿kali)-[~]
└─$ nslookup 74.125.193.99
;; communications error to 192.168.232.100#53: timed out
;; communications error to 192.168.232.100#53: timed out
99.193.125.74.in-addr.arpa      name = di-in-f99.1e100.net.
99.193.125.74.in-addr.arpa      name = ig-in-f99.1e100.net.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ nslookup -querytype=mx google.com
Server:         192.168.232.100
Address:        192.168.232.100#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ nslookup
> set query=ns
> google.com
Server:         192.168.232.100
Address:        192.168.232.100#53

Non-authoritative answer:
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.

Authoritative answers can be found from:
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
> 
```



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use o
Player
1 2 3 4
7:16
kali@kali: ~
File Actions Edit View Help

```
Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ nslookup
> set query=ns
> google.com
Server:         192.168.232.100
Address:        192.168.232.100#53

Non-authoritative answer:
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.

Authoritative answers can be found from:
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
> exit


┌──(kali㉿kali)-[~]
└─$ nslookup -querytype=txt google.com
;; Truncated, retrying in TCP mode.
Server:         192.168.232.100
Address:        192.168.232.100#53

Non-authoritative answer:
google.com      text = "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com      text = "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"
google.com      text = "cisco-ci-domain-verification=479146de172eb01ddee38b1a455ab9e8bb51542ddd7f1fa298557dfa7b22d96
3"
google.com      text = "v=spf1 include:_spf.google.com ~all"
google.com      text = "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com      text = "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com      text = "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com      text = "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com      text = "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com      text = "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      text = "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com      text = "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ 
```

Do note that nslookup can be used on both windows machine and kali linux, We will begin by finding the IP address of a host. To do this, type the following: nslookup www.google.com

As you will see, we are returned with the different IPv4 and IPv6 ip addresses on pic 1 for Google.com. The node, called as “local DNS resolver”, is the first point of contact we make with a DNS query every time.

This is usually the IP address of the device provided to you by your Internet Service Provider. Of course, you can target your “all DNS queries” to a different server by changing your local machine’s network settings accordingly.

We will now perform a reverse lookup which will match an IP address to a domain name. This is also called the DNS PTR record, and can be thought of as the exact opposite of the DNS A record. To do this type: nslookup 74.125.193.99

Oftentimes, we can see that hostnames DNS A and DNS PTR queries do not match on web servers. This is because multiple IP addresses may be matched against a DNS A record to perform load balancing.

We can also find any “Mail eXchange” servers for a particular domain. To do this, type:nslookup -querytype=mx google.com

We can also find the “Name Servers” responsible for a domain. In other words, only those servers which are authoritative sources to keep DNS records of the google.com domain name. To do this, first open an interactive console by typing “nslookup”. Then, type: set query=ns

Then, type the domain name into the terminal.

That is : set query=ns   then google.com or your preferred site.

It is possible to access domain verification data by making a DNS TXT query. nslookup -querytype=txt google.com