Dig Command

- Dig (domain information groper) is a tool that is used for querying DNS servers for various DNS records
- It is very useful for troubleshooting DNS problems.
- Install Dig
- CentOS/RHEL/Fedora
- yum install bind-utils -y
- Debian/Ubuntu
- apt-get install dnsutils -y

Basic DNS Query

- Specify a domain name after the dig command and it will perform a DNS lookup, as shown below
- munees@Munees ~ $ **dig iitmandi.ac.in**
- ; <<>> DiG 9.10.3-P4-Ubuntu <<>> iitmandi.ac.in

;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7553
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:

Output of Command

- Lines beginning with ; are comments not part of the information.
- The first line tell us the version of dig (9.10.3) command.
- Next, dig shows the header of the response it received from the DNS server.
- Next comes the question section, which simply tells us the query, which in this case is a query for the “A” record of **iitmandi.ac.in**. The IN means this is an Internet lookup (in the Internet class).

Reverse DNS Lookup

- we can query an IP address and find the domain name that it points to by querying the PTR record. This is done by using the -x option followed by the IP address to query.
- In the below example we perform a reverse lookup on one of the IP addresses that google.com resolved to in the first example.
- This IP address has one PTR record, pointing to del03s09-in-f14.1e100.net.

```
munees@Munees ~ $ dig -x 172.217.160.238
; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x
172.217.160.238
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status:
NOERROR, id: 48217
;; flags: qr rd ra; QUERY: 1, ANSWER: 1,
AUTHORITY: 4, ADDITIONAL: 9
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;238.160.217.172.in-addr.arpa.    IN PTR
;; ANSWER SECTION:
238.160.217.172.in-addr.arpa. 13924 IN PTR
```

Trace DNS Path

- We can perform a trace on the DNS lookup path with the +trace option.
- First the root name servers for '.' are looked up, followed by the name servers for the .com domain, and then finally the name servers for google.com are returned, followed by the DNS records for it.

```
munees@Munees ~ $  dig google.com +trace

; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com
+trace
;; global options: +cmd
.           170572IN NS   m.root-servers.net.
.           170572IN NS   b.root-servers.net.
.           170572IN NS   a.root-servers.net.
.           170572IN NS   j.root-servers.net.
.           170572IN NS   c.root-servers.net.
.           170572IN NS   l.root-servers.net.
.           170572IN NS   k.root-servers.net.
.           170572IN NS   g.root-servers.net.
.           170572IN NS   i.root-servers.net.
```

Query All DNS Record Types

- We can use the 'ANY' option to query all DNS record types, this way we can quickly see all DNS records available for a domain.
- In the below example we can see the results for all types of different records, including A, AAAA, TXT, MX and NS.

```
;;ANSWER SECTION:
google.com.     129  IN MX   10
aspmx.l.google.com.
google.com.     63IN AAAA
2404:6800:4007:801::200e
google.com.     209  IN A   172.217.26.174
```

Recursive and Iterative DNS Queries

- Recursion in DNS (Domain Name System) is the process of a DNS Server, querying other DNS Server on behalf of original DNS Client.
- Iteration is the process of a DNS Client, making repeated DNS (Domain Name System) Queries to different DNS Servers for name resolution.
- In a Recursive DNS Query, the DNS Client sends a Query to a DNS Server for name resolution. The reply to the DNS Query can be an answer to the query or an error message.

Cont..

- In Recursive DNS Query, If the DNS Server doesn't know the answer to provide accurate answer to the DNS Client.
- DNS Server may query other DNS Servers on behalf of the DNS Client.
- In Iterative DNS Query, when a DNS Client asks the DNS server for name resolution, the DNS Server provides the best answer it has.
- If the DNS Server doesn't know the answer to the DNS Query from Client, the answer can be a reference to another lower level DNS Server