

Group:
Essential Group

Foundations of Digital Investigation

Report Number:
Report No. 5

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Date of Task Assignment :

1/5/2026

Due Date:
1/6/2026

Scenario: You are a junior IT support technician at a tech company. Your manager asks you to verify the domain settings for earthlink.iq because employees are reporting issues receiving emails.

Question 1: What system will you use to translate the domain name earthlink.iq into an IP address that a computer can understand?

ANSWER

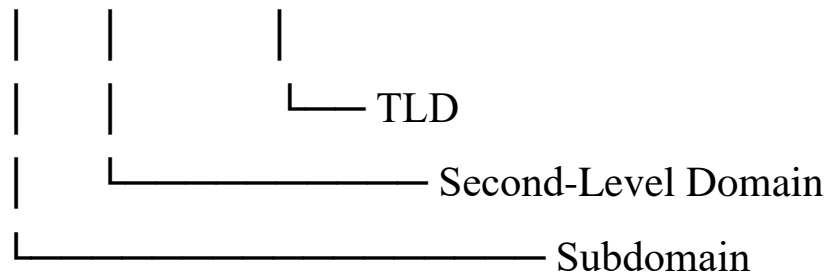
DNS : it translates human-readable domain names into machine-readable IP address

Question 2: In the domain mirror.earthlink.iq, what is the .iq portion called?

ANSWER

The **.iq** portion is a Country Code Top-Level Domain (TLD)

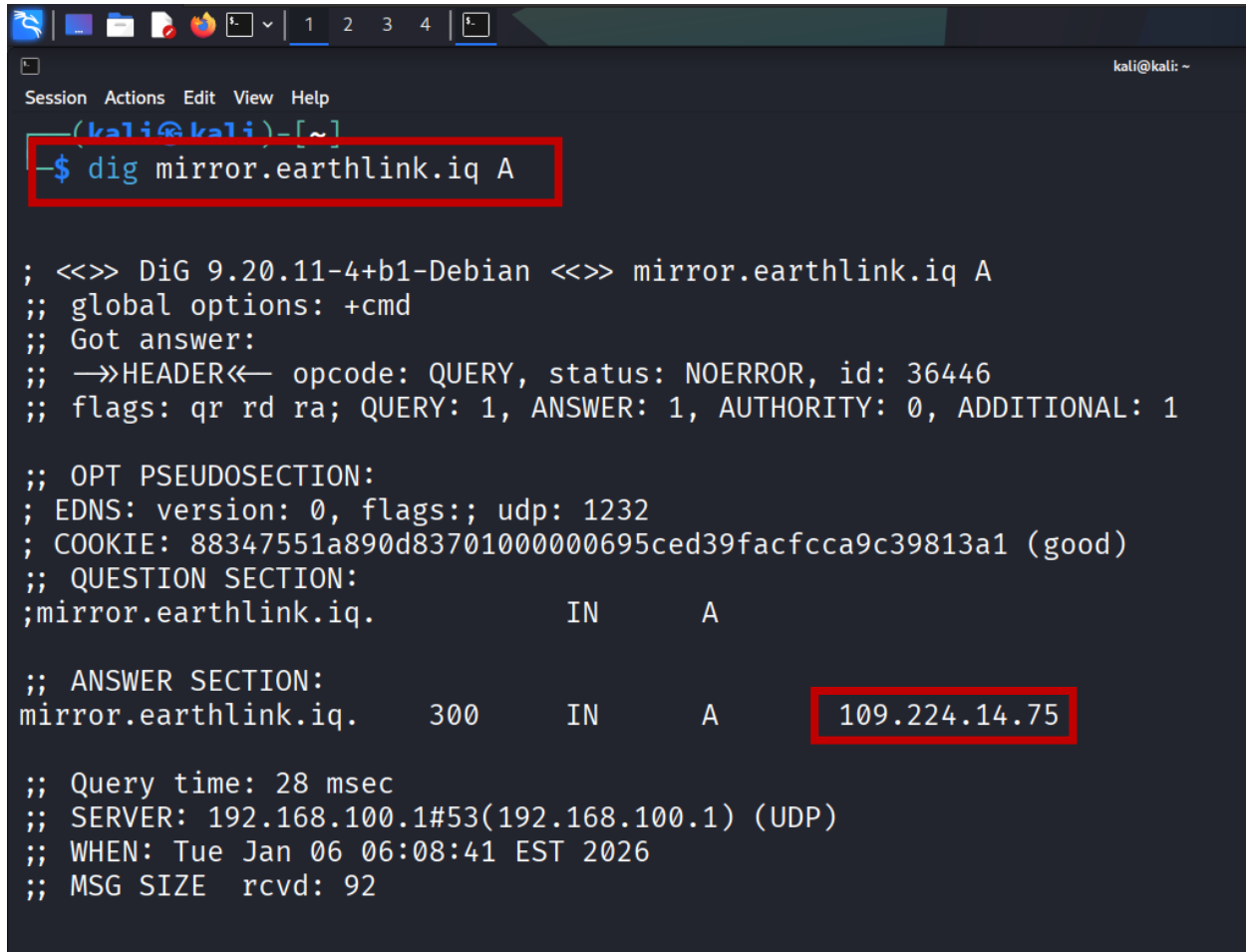
mirror.earthlink.iq



Question 3: Use the dig tool to find the IPv4 address of mirror.earthlink.iq. Which record type are you looking for?

ANSWER

Ipv4 represents A record



```
Session Actions Edit View Help
(kali@kali)-[~]
└─$ dig mirror.earthlink.iq A

; <<>> DiG 9.20.11-4+b1-Debian <<>> mirror.earthlink.iq A
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 36446
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 88347551a890d83701000000695ced39facfcca9c39813a1 (good)
;; QUESTION SECTION:
;mirror.earthlink.iq.                IN      A

;; ANSWER SECTION:
mirror.earthlink.iq.    300     IN      A      109.224.14.75

;; Query time: 28 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Tue Jan 06 06:08:41 EST 2026
;; MSG SIZE rcvd: 92
```

Figure 1 shows the dig command to find the ipv4

Question 4: The company is having email issues. Which record type must you check to ensure emails are being routed to the correct servers?

ANSWER

The MX record

```
(kali@kali)-[~]
└─$ dig earthlink.iq MX

; <<>> DiG 9.20.11-4+b1-Debian <<>> earthlink.iq MX
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 47273
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1232
; COOKIE: 77d226d9b440a6ad01000000695cee2eedd6d2d68f1811c6 (good)
;; QUESTION SECTION:
;earthlink.iq.                IN      MX

; ANSWER SECTION:
earthlink.iq.                300     IN      MX      10 elcld-mx2.titanhq.com.
earthlink.iq.                300     IN      MX      5  elcld-mx1.titanhq.com.

;; Query time: 32 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Tue Jan 06 06:12:46 EST 2026
;; MSG SIZE rcvd: 132
```

Figure 2 shows the dig command to find the emails

Question 5: While using dig, you see a TTL value of 300. What does this indicate?

ANSWER

1. TTL is abbreviation of Time To Live of 300 seconds means the DNS record can be cached for 5 minutes
2. TTL controls how long DNS responses are stored by resolvers
3. Lower TTL values are used when frequent changes are expected
4. After expiration, resolvers must re-query authoritative DNS servers
5. Short TTL = faster propagation of changes Long TTL = better performance, slower updates