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 addresse

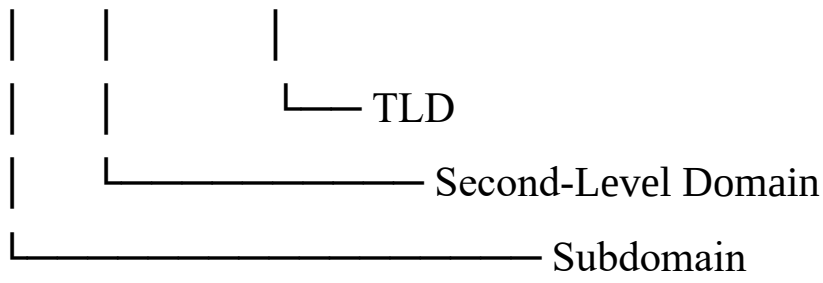
---

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

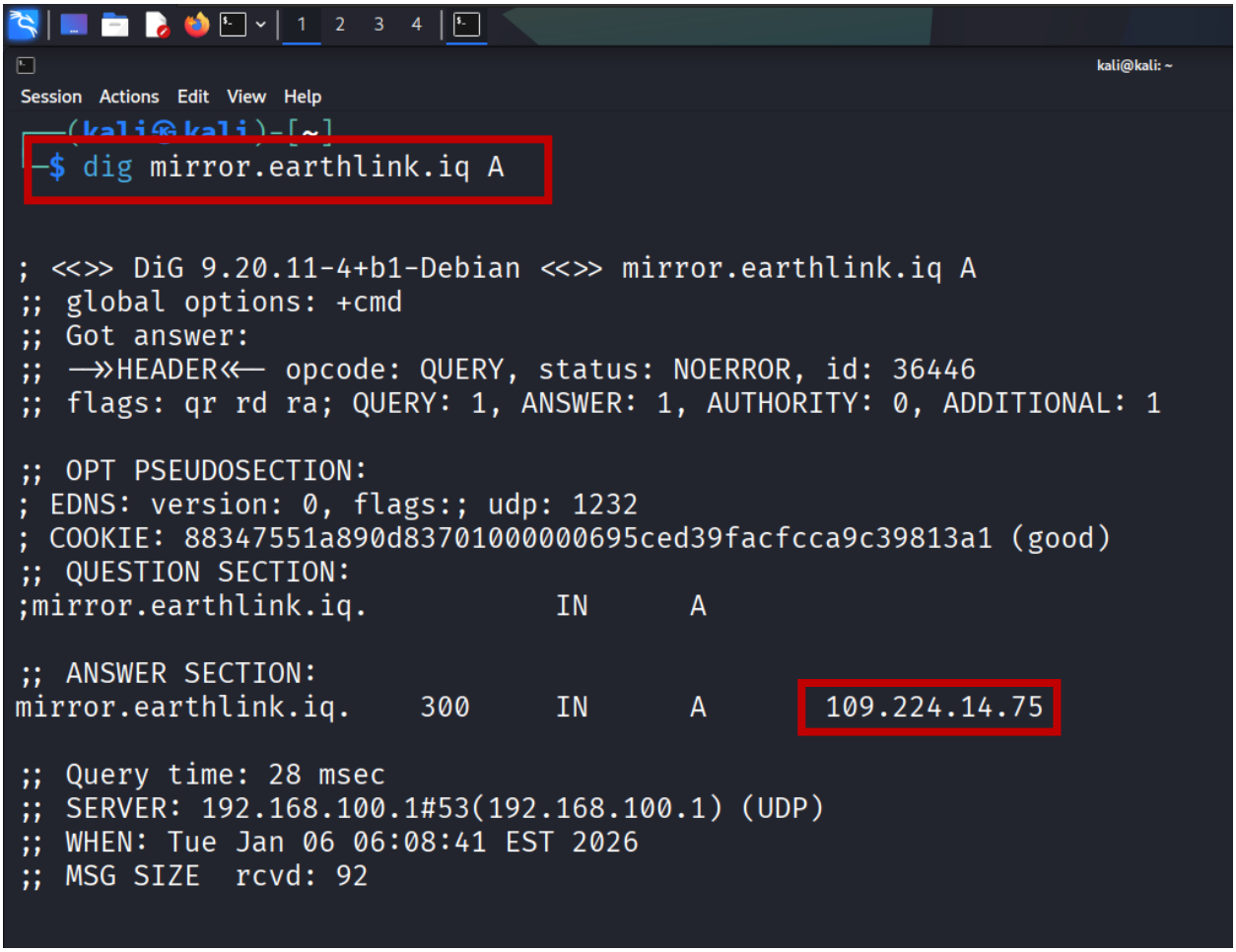


Figure 1 shows the dig command to find the ipv4

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

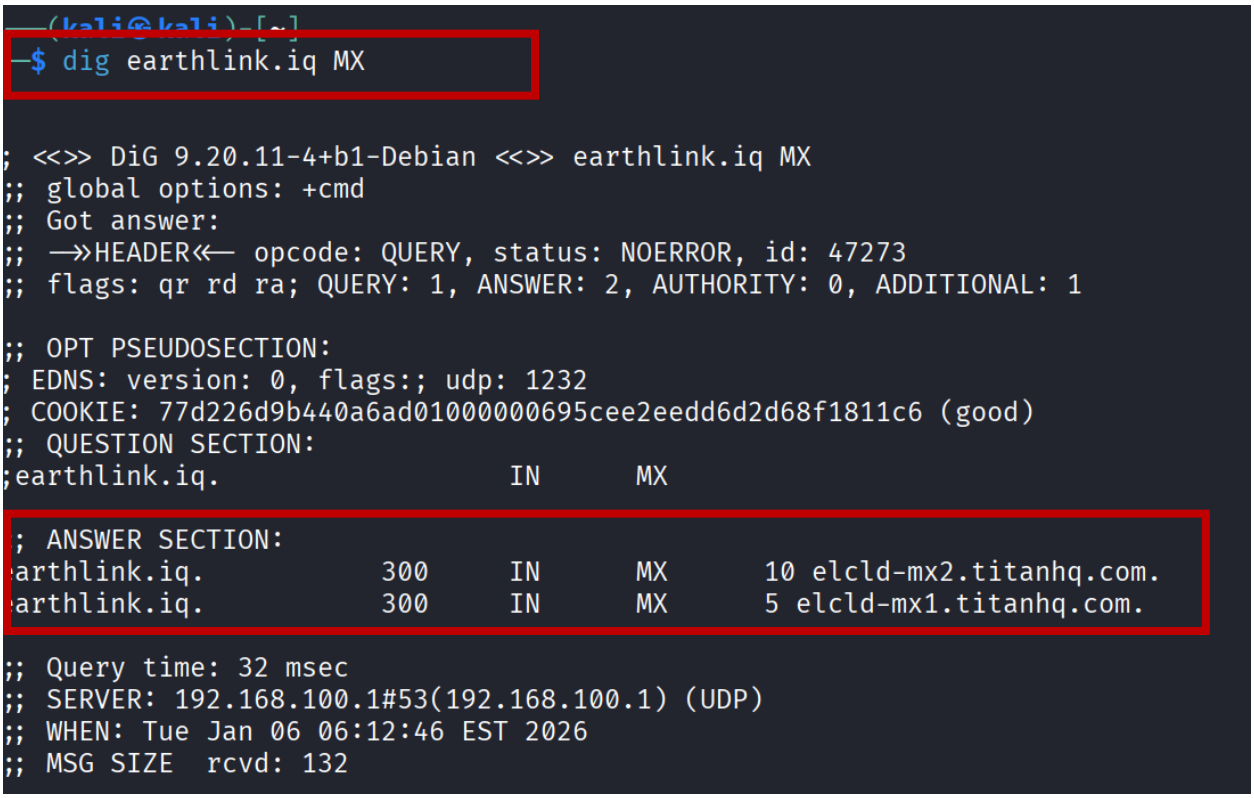


Figure 2 shows the dig command to find the emails

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