Assignment Number: 6

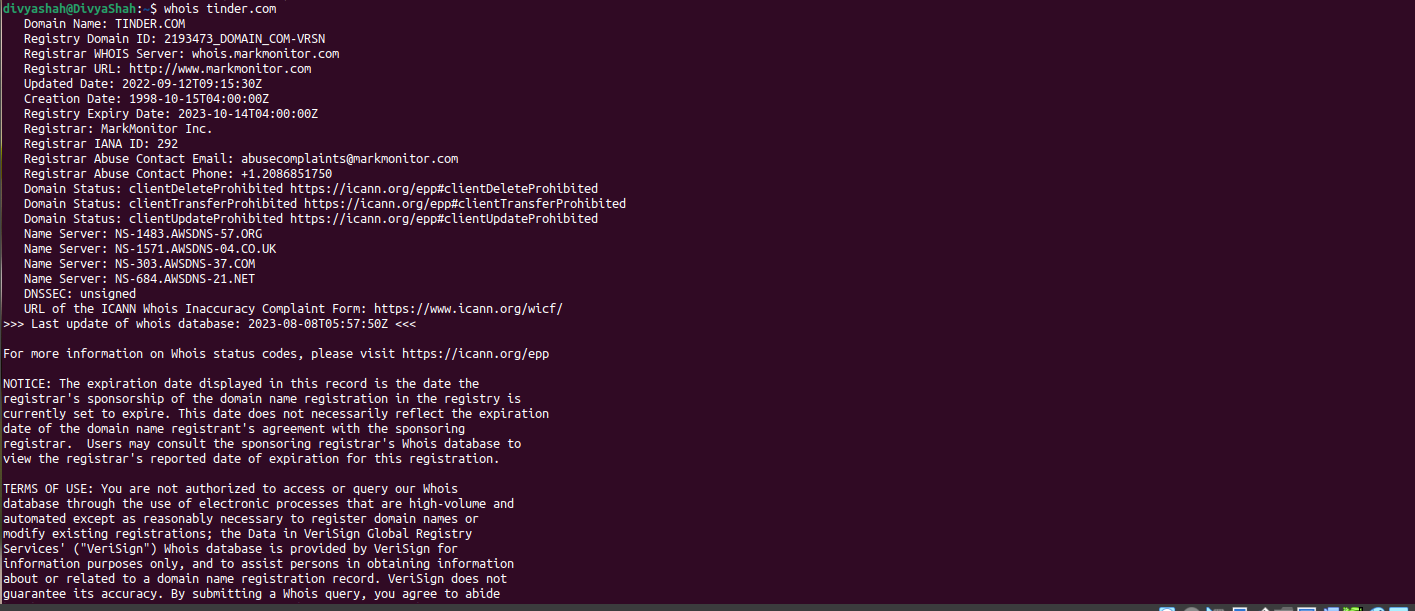
Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 24/08/2023

**Aim:** Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookupt, nikto, dmitry to gather information about networks and domain registrars.

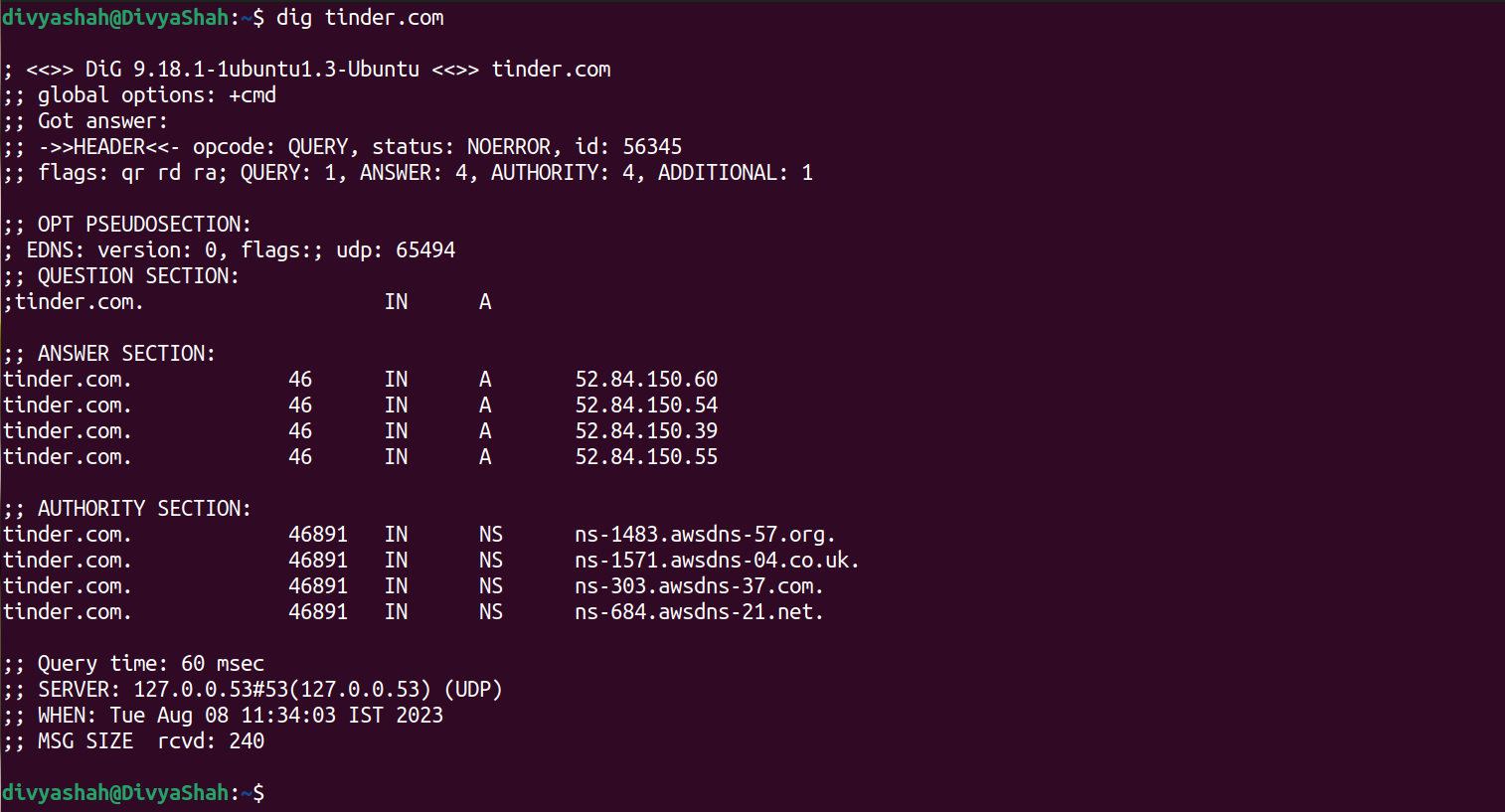
**LO mapped:** LO3

**Theory:**

The whois command is used to retrieve information about domain names, IP addresses, and their associated registrants, contacts, and more.

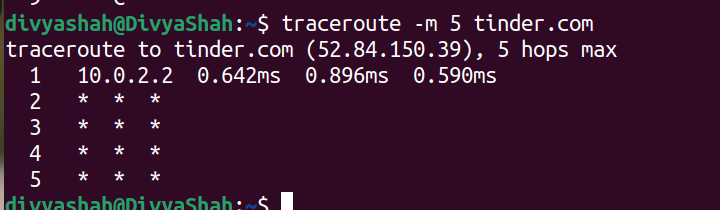
This command to retrieve basic information about a domain name

The dig command is a powerful tool for querying DNS (Domain Name System) servers to retrieve information about domain names, IP addresses, and various DNS records.



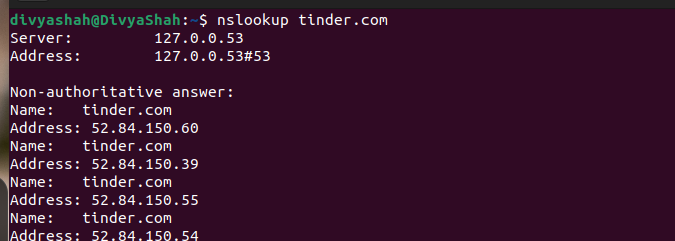
To perform a basic DNS lookup for a domain name

The traceroute command is used to trace the route that packets take from your computer to a destination IP address or domain name. It shows you each hop (router) that the packet passes through on its way to the destination.



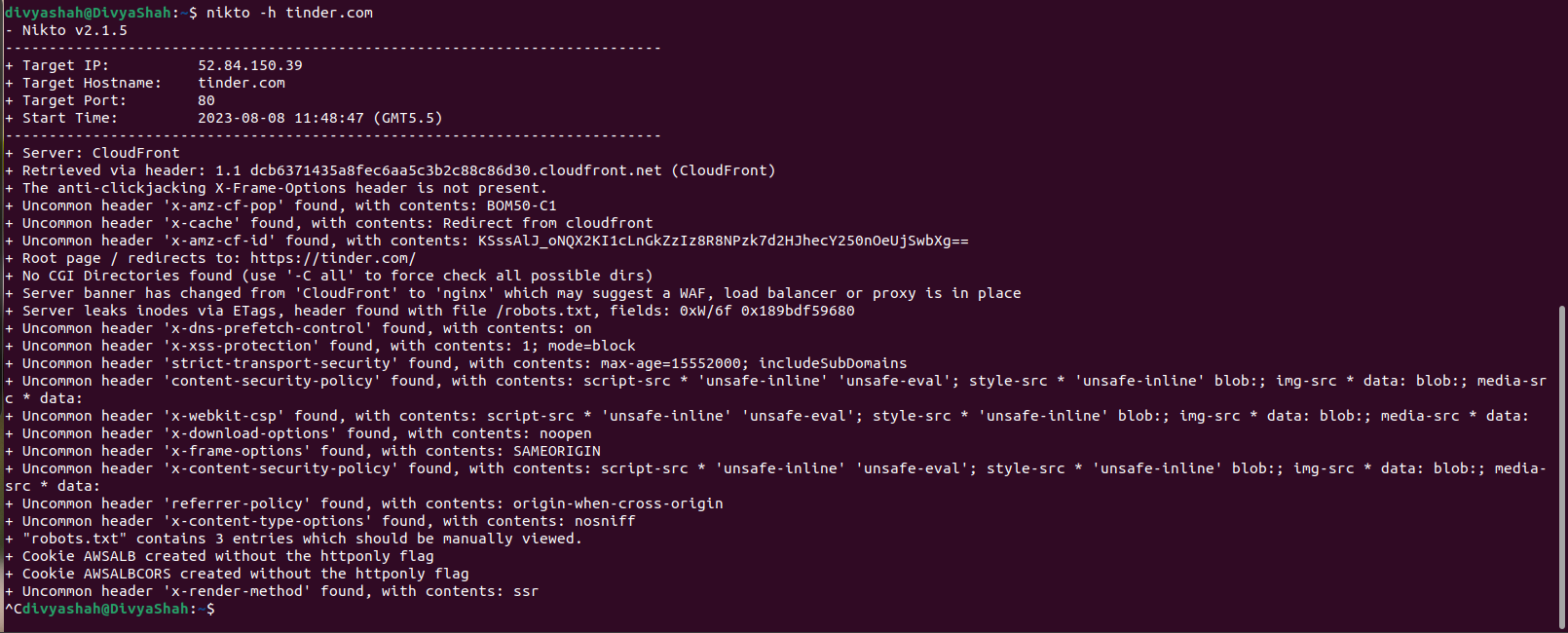
To specify the number of hops (maximum TTL value) using the -m option

The nslookup command is used to query DNS (Domain Name System) servers to retrieve information about domain names, IP addresses, and related DNS records.

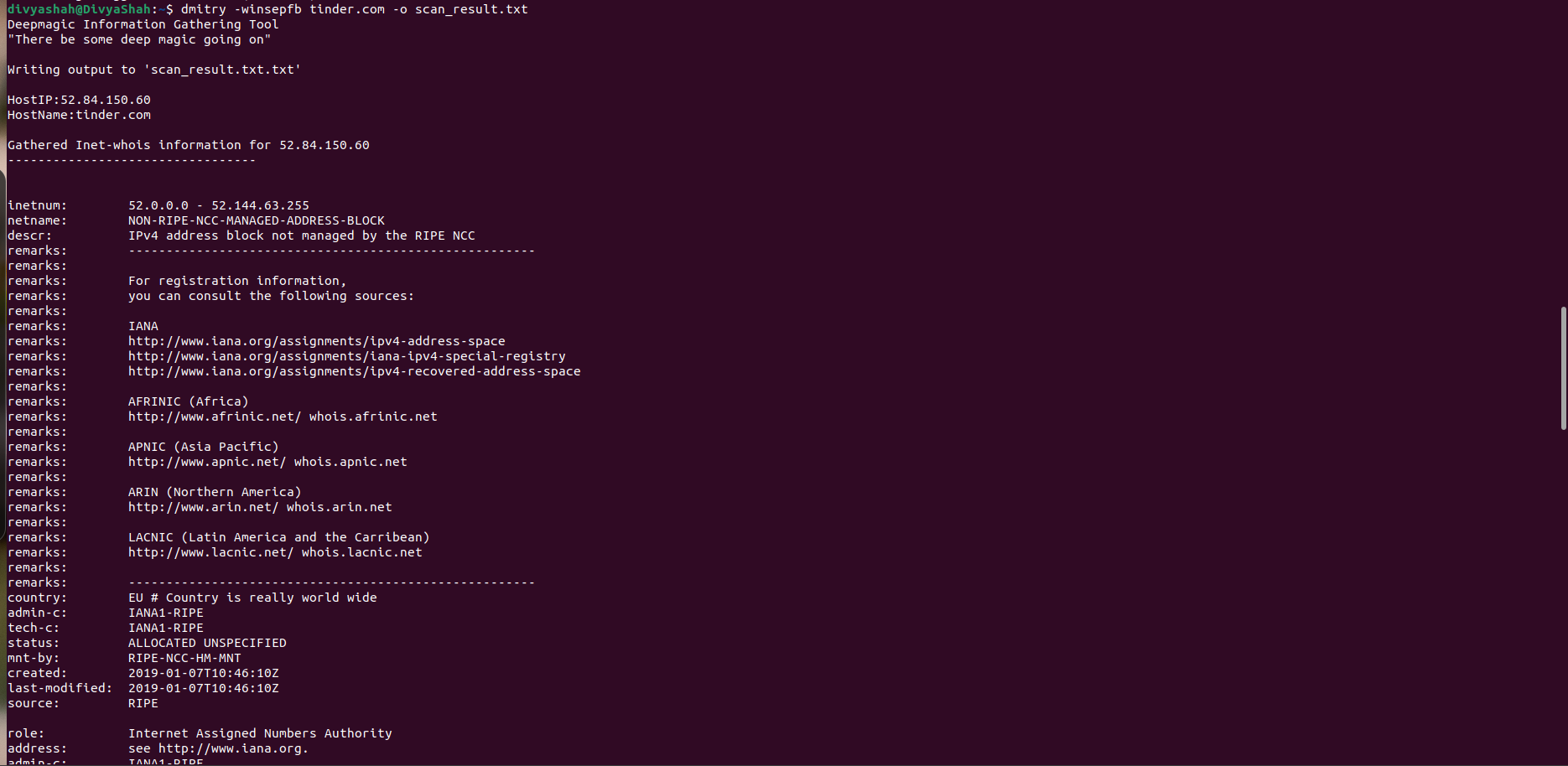


To perform a basic DNS lookup for a domain name

Nikto is a web server vulnerability scanner that helps you identify security vulnerabilities and potential issues on web servers.



DMitry (Deepmagic Information Gathering Tool) is a command-line tool used for information gathering about a target. It can retrieve a variety of information about a domain, IP address, or hostname.



Conclusion: By this assignment we understand use of various network reconnaissance tools.