Find A record of the domain
dig A example.com
Find NS record of the domain
dig NS example.com
Find SOA record fo the domain (know primary dns server of the domain)
dig SOA example.com
Find A record of the primary NS server
dig A primary.ns.server.of.example.com
Try zone transfer of example.com
dig axfr @primary_ns_server_ip_address example.com

IP logger:
Grabify
Choose interesting content for the target, such as a funny meme.
Enter the meme's link in Grabify, and it will generate a compressed URL that you can use and a tracking code. Copy both.
Send the target's compressed link and when they open it, go back to Grabify and enter the tracking code into the search box on the homepage. The application will show you a person's IP address and other interesting information.

An IP address (Internet Protocol address) can provide various types of information, including:

Geolocation (Location of the device (city or coordinates,The area code for that region)):
ISP (Internet Service Provider) and organization's name:
Network Type:
Hostname:
ASN (Autonomous System Number):
Open Ports and Any known services running:
Historical Data:
Domains hosted at that IP:

IP Address can reveal the geolocation and network details of a target, aiding in the identification of potential vulnerabilities or tracing the source of online activities. By analysing IP addresses found in open sources, OSINT practitioners can gather valuable insights about individuals, organisations, or entities operating on the internet.

Geolocation: You can determine the approximate physical location of the IP address. This includes the country, region, city, and even the latitude and longitude coordinates. (You can find the network the address belongs to)
Tools
ipfingerprints.com
ipinfo.io
Iprover

Iptraker
https://ipfind.com
https://securitytrails.com/
https://viewdns.info/
WHOIS Lookup:
https://www.whois.com
https://who.is
https://in.godaddy.com/whois
https://www.whoxy.com/
https://viewdns.info/whois/
https://virustotal.com
https://netcraft.com
Reverse DNS Lookup:
https://viewdns.info/reversewhois/
https://www.reversewhois.io/
https://www.whoxy.com/reverse-whois
https://securitytrails.com/
ASN Lookup:
https://mxtoolbox.com/asn.aspx
https://hackertarget.com/as-ip-lookup/
Ip address and domain information plugin
Sublist3r
Amass
Subfinder
Findomain
python sublist3r.py -d example.com
amass enum -d example.com
subfinder -d example.com
findomain -t example.com
NMAP
nmap -p- target_ip_or_hostname
nmap -p 80,443 target_ip_or_hostname
nmap -sT -sV -sC -A -O -p 80,443 target_ip_or_hostname target_ip_or_hostname
nmap --script script_name target_ip_or_hostname

ISP (Internet Service Provider) and organization's name: You can identify the company that provides internet services to the IP address. This can give you an idea of the type of network the IP address is on.

You can define the internet service provider of this IP address and in some cases, getting in touch with the ISP you can even get the physical address of your target;

Network Type: You can sometimes infer whether the IP address is associated with a residential, business, or data center network based on the ISP and other information.

Hostname: You can resolve the IP address to find the associated domain name (hostname). This can provide information about the website or service associated with the IP.
When you perform a reverse DNS lookup, you are essentially asking for the PTR record associated with a particular IP address. The PTR record helps in identifying the hostname or domain name linked to that IP address.

ASN (Autonomous System Number): You can determine the unique identifier for the network or organization that owns or controls the IP address. This is useful for understanding the network infrastructure.

Open Ports: By scanning the IP address, you can identify which ports are open and potentially infer which services or applications are running.

Historical Data: Some IP address lookup tools may provide historical information about the IP's activity, such as past uses or incident