Information Gathering Tool

- PROJECT REPORT
- SUBMITTED BY – Harshit Sharma
- EMAIL ID- hs02121980@gmail.com

Objective

The main objective of this project was to create a simple tool using Python that can fetch the IP address and location of any website provided by the user. The idea was to understand how information gathering works during the initial phase of cybersecurity and how APIs can be used to extract details in a structured format like JSON.

Tools and Technologies Used

To complete this project, I used the following tools and technologies:

- **Programming Language:** Python
- **Libraries Used:**
  - **.sys**
  - .socket
  - .request
  - .json
- **API Used:** ipinfo.in
- **Operating System:** Kali Linux

How the Tool will work?

•The user provides a website name in the command line using a simple syntax:

python infotool.py <**websiteurl**>

•The script first resolves the IP address of the website using the **socket library**.

•Once the IP is obtained, it sends a request to **ipinfo.io API to get the location details**.

•The response from the API is in JSON format and is printed in a clean, readable format using **json.dumps()**

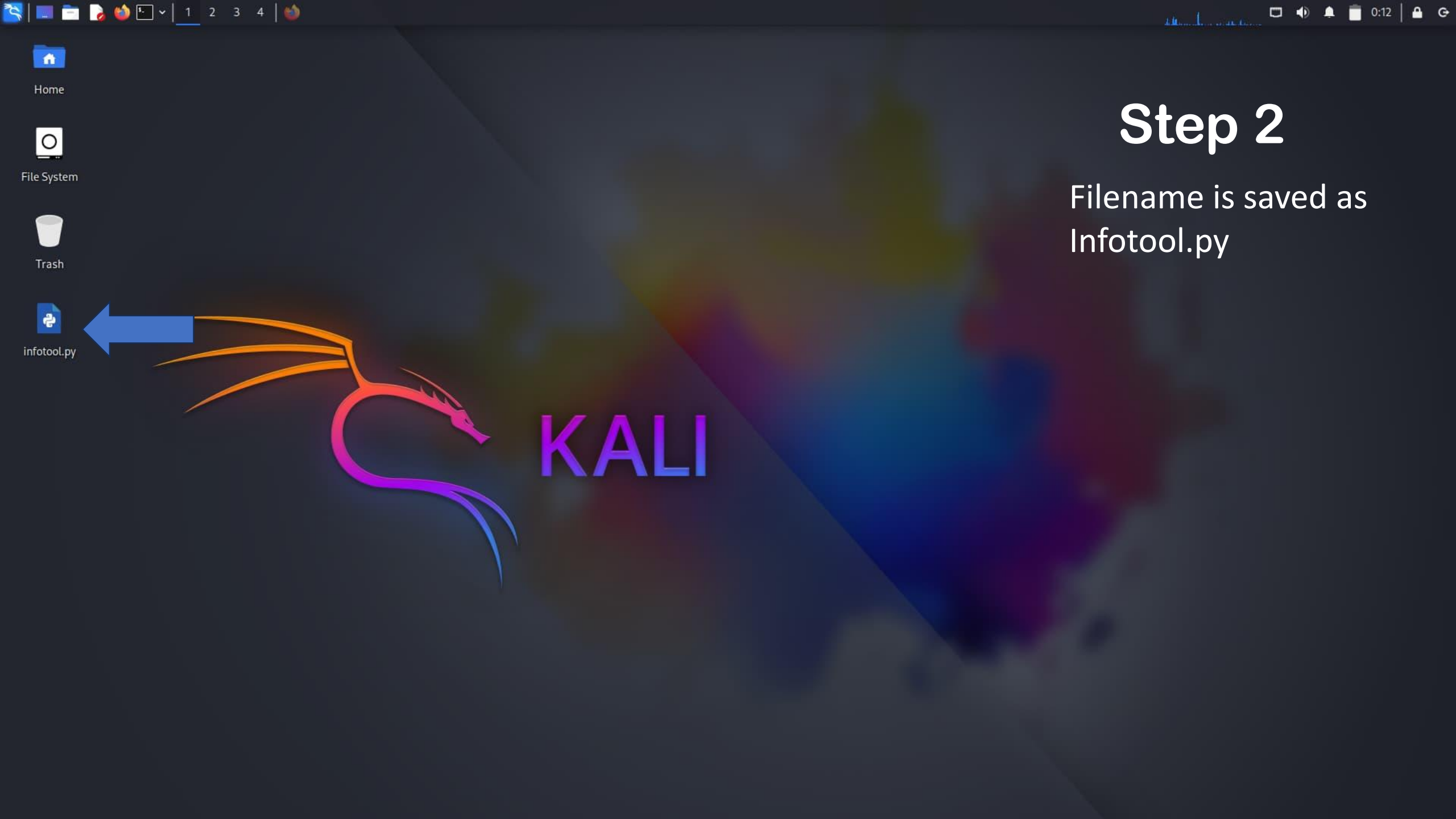
~/Desktop/infotool.py - Mousepad

File Edit Search View Document Help

```
import sys
import socket
import requests
import json

def get_ip(website_url):
    try:
        ip = socket.gethostbyname(website_url)
        return ip
    except socket.gaierror:
        print("Unable to get IP address. Check the URL.")
        sys.exit()

def get_location_info(ip):
    try:
        response = requests.get(f"https://ipinfo.io/{ip}/json")
        data = response.json()
        return data
    except requests.RequestException:
        print("Error fetching location info.")
        sys.exit()

def main():
    if len(sys.argv) != 2:
        print("Usage: python infotool.py <websiteurl>")
        sys.exit()

    website_url = sys.argv[1]
    ip_address = get_ip(website_url)
    print(f"\nIP Address of {website_url}: {ip_address}")

    location_info = get_location_info(ip_address)
    print("\nLocation Information (in JSON):")
    print(json.dumps(location_info, indent=4))

if __name__ == "__main__":
    main()
```

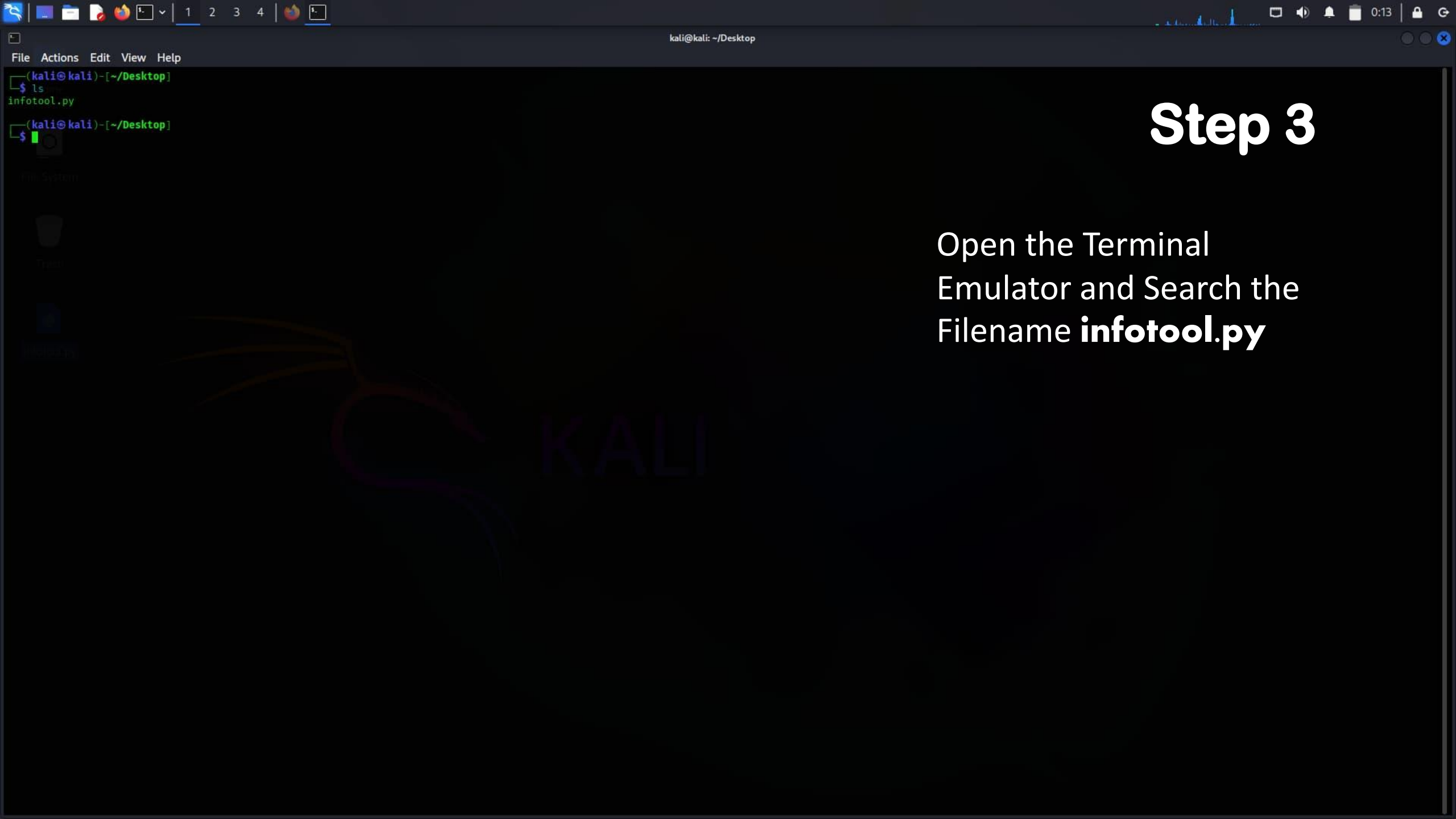
Step 1

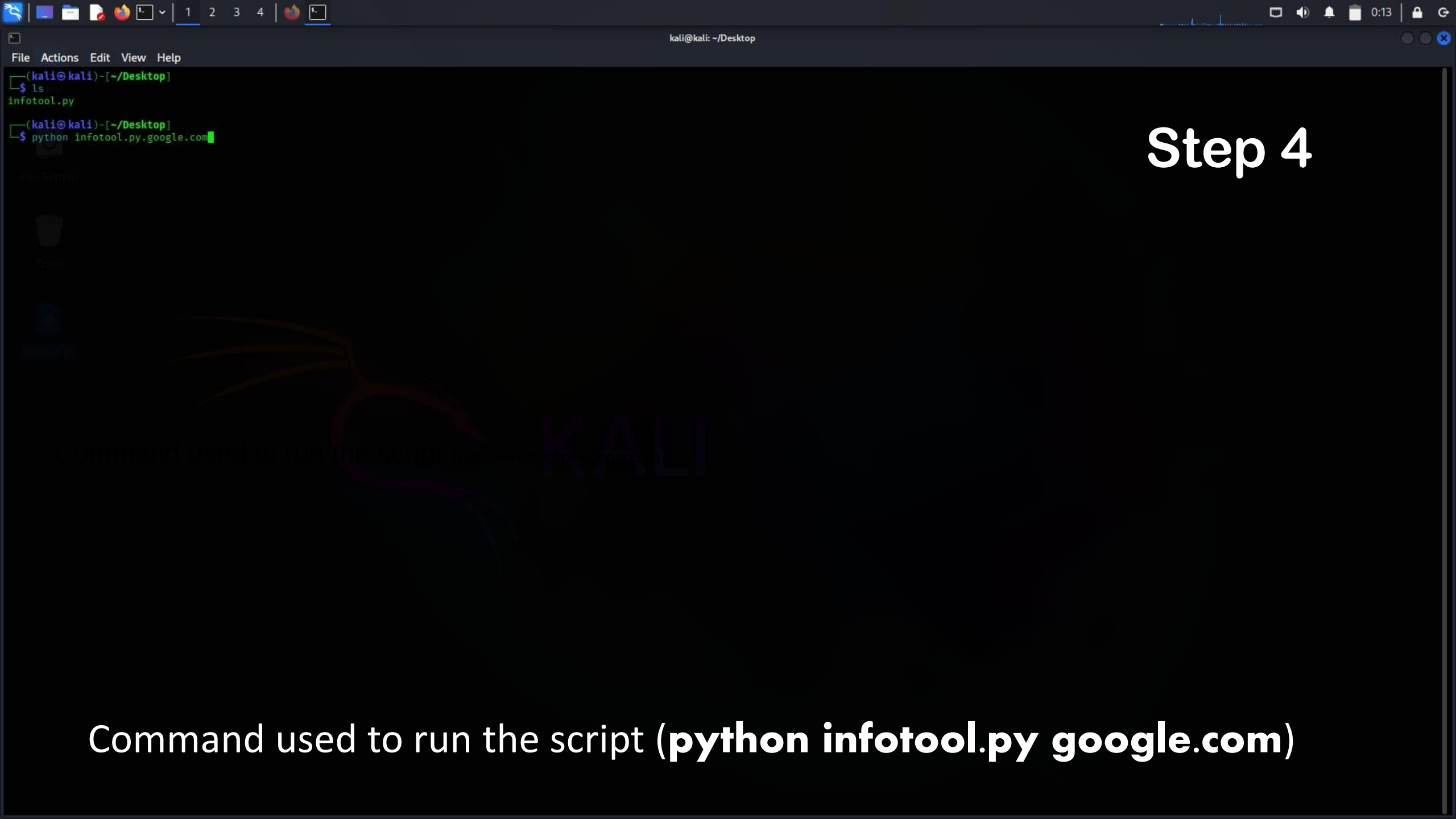
Python code written in terminal or editor and Saving the filename as infotool.py

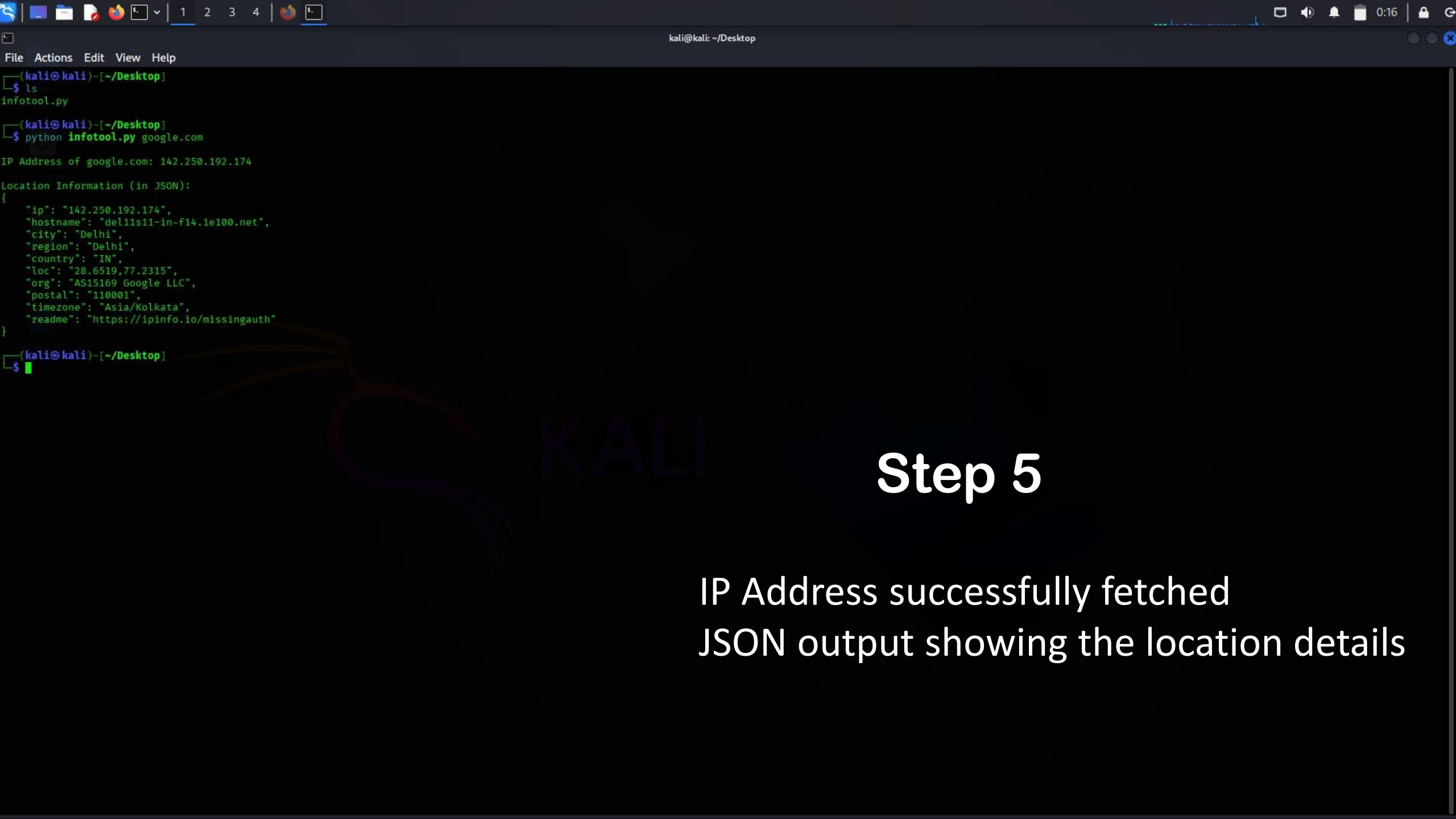


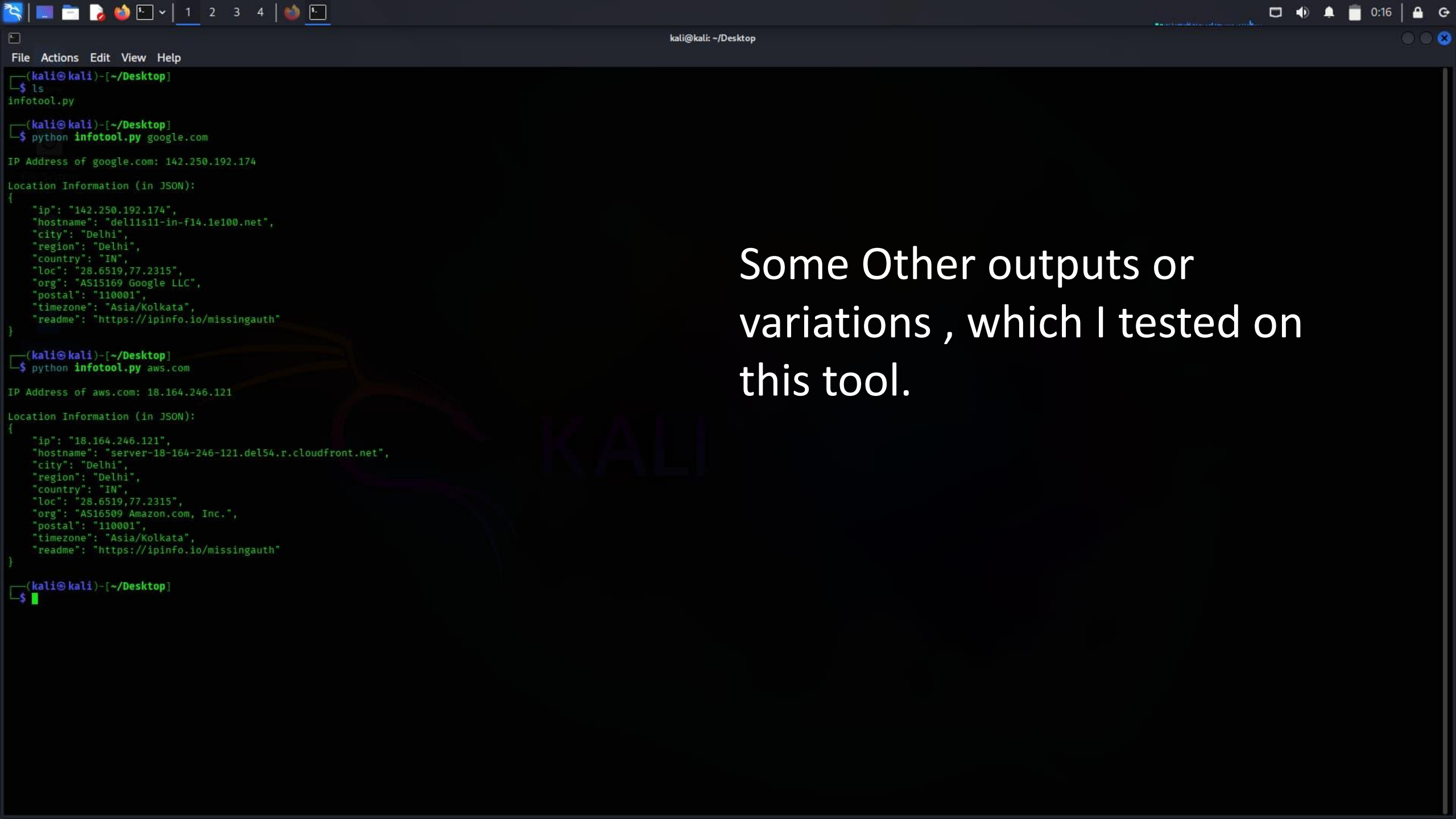
Step 2

Filename is saved as Infotool.py


kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ ls
infotool.py
(kali㉿kali)-[~/Desktop]
$
Step 3
Open the Terminal Emulator and Search the Filename infotool.py


kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ ls
infotool.py
(kali㉿kali)-[~/Desktop]
$ python infotool.py.google.com
Step 4
Command used to run the script (python infotool.py google.com)


kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ ls
infotool.py
(kali㉿kali)-[~/Desktop]
$ python infotool.py google.com
IP Address of google.com: 142.250.192.174
Location Information (in JSON):
{
"ip": "142.250.192.174",
"hostname": "del11s11-in-f14.1e100.net",
"city": "Delhi",
"region": "Delhi",
"country": "IN",
"loc": "28.6519,77.2315",
"org": "AS15169 Google LLC",
"postal": "110001",
"timezone": "Asia/Kolkata",
"readme": "https://ipinfo.io/missingauth"
}
(kali㉿kali)-[~/Desktop]
$
Step 5
IP Address successfully fetched
JSON output showing the location details



Some Other outputs or variations , which I tested on this tool.

```
infotool.py

┌──(kali㉿kali)-[~/Desktop]
└─$ python infotool.py google.com

IP Address of google.com: 142.250.192.174

Location Information (in JSON):
{
    "ip": "142.250.192.174",
    "hostname": "del11s11-in-f14.1e100.net",
    "city": "Delhi",
    "region": "Delhi",
    "country": "IN",
    "loc": "28.6519,77.2315",
    "org": "AS15169 Google LLC",
    "postal": "110001",
    "timezone": "Asia/Kolkata",
    "readme": "https://ipinfo.io/missingauth"
}

┌──(kali㉿kali)-[~/Desktop]
└─$ python infotool.py aws.com

IP Address of aws.com: 18.164.246.121

Location Information (in JSON):
{
    "ip": "18.164.246.121",
    "hostname": "server-18-164-246-121.del54.r.cloudfront.net",
    "city": "Delhi",
    "region": "Delhi",
    "country": "IN",
    "loc": "28.6519,77.2315",
    "org": "AS16509 Amazon.com, Inc.",
    "postal": "110001",
    "timezone": "Asia/Kolkata",
    "readme": "https://ipinfo.io/missingauth"
}

┌──(kali㉿kali)-[~/Desktop]
└─$ python infotool.py microsoft.com

IP Address of microsoft.com: 13.107.253.48

Location Information (in JSON):
{
    "ip": "13.107.253.48",
    "city": "Redmond",
    "region": "Washington",
    "country": "US",
    "loc": "47.6740,-122.1215",
    "org": "AS8075 Microsoft Corporation",
    "postal": "98052",
    "timezone": "America/Los_Angeles",
    "readme": "https://ipinfo.io/missingauth",
    "anycast": true
}

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Conclusion-

- Through this mini project, I got a better understanding of how basic information gathering works using Python. I learned how to resolve domains to IPs, interact with public APIs, handle JSON responses, and format data neatly for the user. It was a helpful experience that also gave me some exposure to the early stages of cybersecurity.

- **THANK YOU**