TOOL NAME : information-tool.py

Abstract :

This project describes the development of a Python information gathering tool. The tool, named "information-tool.py", extracts website details such as

**** IP address,***

****Domain name,***

****Location (city, region, country),***

****Organization, and time zone by leveraging publicly available resources.***

****

Objective :

The objective of this project was to design a Python program that gathers information about a website using its domain name or URL.

****

Introduction :

Information gathering is a crucial initial step in various tasks, including network security assessments and web-based research. This tool automates the process of collecting publicly available information about a website.

****

Methodology :

The Python script utilizes the requests and socket libraries to interact with websites and retrieve data. Here's a breakdown of the steps involved:

1. ***User Input: The user provides the target website's domain name or URL as a command-line argument.***
2. ***Domain Name Extraction: The script extracts the domain name.***
3. ***IP Address Lookup: The script uses the socket.gethostbyname() function to retrieve the IP address associated with the domain name.***
4. ***Information Retrieval: The script leverages the requests library to send a GET request to an IP info service (like https://ipinfo.io) using the retrieved IP address.***
5. ***Data Parsing: The script parses the JSON response from the IP info service to extract details such as location (city, region, country), organization, and time zone.***
6. ***Output: The script presents the gathered information in a user-friendly format on the console.***

Screenshots:

1.Program (Python Script)

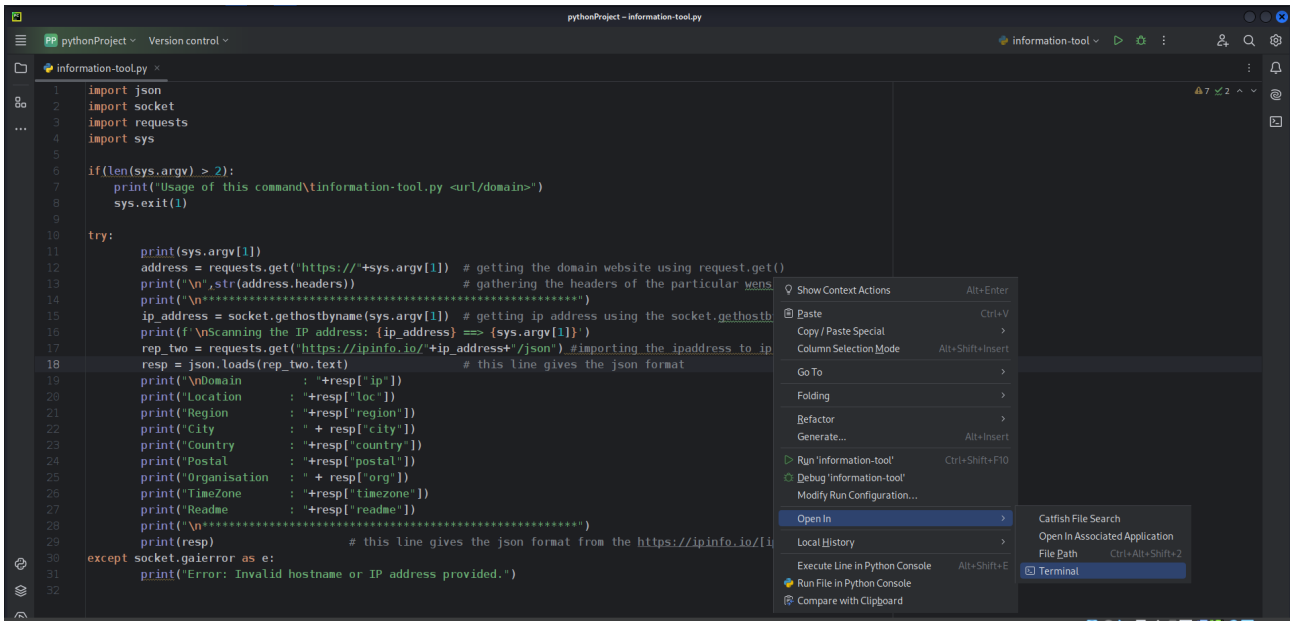
```python
import json
import socket
import requests
import sys

if(len(sys.argv) > 2):
    print("Usage of this command\tinformation-tool.py <url/domain>")
    sys.exit(1)

try:
        print(sys.argv[1])
        address = requests.get("https://"+sys.argv[1])  # getting the domain website using request.get()
        print("\n",str(address.headers))                # gathering the headers of the particular wensite
        print("\n*******************************************************")
        ip_address = socket.gethostbyname(sys.argv[1])  # getting ip address using the socket.gethostbyname()
        print(f'\nScanning the IP address: {ip_address} ==> {sys.argv[1]}')
        rep_two = requests.get("https://ipinfo.io/"+ip_address+"/json") #importing the ipaddress to ipinfo.io website
        resp = json.loads(rep_two.text)                 # this line gives the json format
        print("\nDomain         : "+resp["ip"])
        print("Location       : "+resp["loc"])
        print("Region         : "+resp["region"])
        print("City           : " + resp["city"])
        print("Country        : "+resp["country"])
        print("Postal         : "+resp["postal"])
        print("Organisation   : " + resp["org"])
        print("TimeZone       : "+resp["timezone"])
        print("Readme         : "+resp["readme"])
        print("\n*******************************************************")
        print(resp)                     # this line gives the json format from the https://ipinfo.io/[ipaddress]/json
except socket.gaierror as e:
        print("Error: Invalid hostname or IP address provided.")
```

Here is the python program that is used to get the ip address and location(country, region) as given i additionally added for realistic information provided with City, Postal and TimeZone.

2.Opening terminal



So , Right click and go to "Open In" option , left click the option and get noticed on Terminal by using this option we can open the Terminal and give the ipaddress/domain_name as Argument.

3.Compiling :

```
Terminal    Local (3)
┌──(.venv)─(kali㉿kali)-[~/PycharmProjects/pythonProject]
└─$ python information-tool.py youtube.com
youtube.com

 {'Content-Type': 'text/html; charset=utf-8', 'X-Content-Type-Options': 'nosniff', 'Cache-Control': 'no-ca
che, no-store, max-age=0, must-revalidate', 'Pragma': 'no-cache', 'Expires': 'Mon, 01 Jan 1990 00:00:00 GM
T', 'Date': 'Mon, 20 May 2024 09:16:14 GMT', 'X-Frame-Options': 'SAMEORIGIN', 'Strict-Transport-Security':
 'max-age=31536000', 'Permissions-Policy': 'ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-ful
l-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-form-factor=*, ch-ua-platform=*, ch-ua-platform-vers
ion=*', 'Origin-Trial': 'AmhMBR6zCLzDDxpW+HfpP67BqwIknWnyMOXOQGfzYswFmJe+fgaI6XZgAzcxOrzNtP7hEDsOo1jdjFnVr
2IdxQ4AAAB4eyJvcmlnaW4iOiJodHRwczovL3lvdXRlYmUuY29tOjQ0MyIsImZlYXRlcmUiOiJXZWJWaWV3WFJlcXVlc3RlZFdpdGhEZXB
yZWNhdGlvbiIsImV4cGlyeSI6MTc1ODA2NzE5OSwiaXNTdWJkb21haW4iOnRydWV9', 'Cross-Origin-Opener-Policy': 'same-or
igin-allow-popups; report-to="youtube_main"', 'Report-To': '{"group":"youtube_main","max_age":2592000,"end
points":[{"url":"https://csp.withgoogle.com/csp/report-to/youtube_main"}]}', 'P3P': 'CP="This is not a P3P
 policy! See http://support.google.com/accounts/answer/151657?hl=en-GB for more info."', 'Content-Encoding
': 'gzip', 'Server': 'ESF', 'X-XSS-Protection': '0', 'Set-Cookie': 'GPS=1; Domain=.youtube.com; Expires=Mo
n, 20-May-2024 09:46:14 GMT; Path=/; Secure; HttpOnly, YSC=2dDO1HATlK0; Domain=.youtube.com; Path=/; Secur
e; HttpOnly; SameSite=none, VISITOR_INFO1_LIVE=r3t94tBhEzE; Domain=.youtube.com; Expires=Sat, 16-Nov-2024
09:16:14 GMT; Path=/; Secure; HttpOnly; SameSite=none, VISITOR_PRIVACY_METADATA=CgJJThIEGgAgTw%3D%3D; Doma
in=.youtube.com; Expires=Sat, 16-Nov-2024 09:16:14 GMT; Path=/; Secure; HttpOnly; SameSite=none', 'Alt-Svc
': 'h3=":443"; ma=2592000,h3-29=":443"; ma=2592000', 'Transfer-Encoding': 'chunked'}

*******************************************************

Scanning the IP address: 142.250.194.142 ==> youtube.com

Domain         : 142.250.194.142
Location       : 28.6519,77.2315
Region         : Delhi
City           : Delhi
Country        : IN
Postal         : 110001
Organisation   : AS15169 Google LLC
TimeZone       : Asia/Kolkata
Readme         : https://ipinfo.io/missingauth

*******************************************************
{'ip': '142.250.194.142', 'hostname': 'del12s05-in-f14.1e100.net', 'city': 'Delhi', 'region': 'Delhi', 'co
untry': 'IN', 'loc': '28.6519,77.2315', 'org': 'AS15169 Google LLC', 'postal': '110001', 'timezone': 'Asia
/Kolkata', 'readme': 'https://ipinfo.io/missingauth'}

┌──(.venv)─(kali㉿kali)-[~/PycharmProjects/pythonProject]
└─$
```

So this is Complied and Executed part,

In this we compile and execute the program by formatted as

"python information-tool.py [URL/domain]" this shoes output of

1.domain-name

2.domain-headers

3.Scanning of ipaddress and related information of domain from the ipinfo.io

4.JSON format of domain in ipinfo.io

4.Full layout:

information-tool.py

```python
import json
import socket
import requests
import sys

if(len(sys.argv) > 2):
    print("Usage of this command\tinformation-tool.py <url/domain>")
    sys.exit(1)

try:
        print(sys.argv[1])
        address = requests.get("https://"+sys.argv[1])  # getting the domain website using request
        print("\n",str(address.headers))                # gathering the headers of the particular w
        print("\n*******************************************************")
        ip_address = socket.gethostbyname(sys.argv[1])  # getting ip address using the socket.getho
        print(f'\nScanning the IP address: {ip_address} ==> {sys.argv[1]}')
        rep_two = requests.get("https://ipinfo.io/"+ip_address+"/json") #importing the ipaddress to
        resp = json.loads(rep_two.text)                 # this line gives the json format
        print("\nDomain         : "+resp["ip"])
        print("Location       : "+resp["loc"])
        print("Region         : "+resp["region"])
        print("City           : " + resp["city"])
        print("Country        : "+resp["country"])
        print("Postal         : "+resp["postal"])
        print("Organisation   : " + resp["org"])
        print("TimeZone       : "+resp["timezone"])
        print("Readme         : "+resp["readme"])
        print("\n*******************************************************")
        print(resp)                     # this line gives the json format from the https://ipinfo.io
except socket.gaierror as e:
        print("Error: Invalid hostname or IP address provided.")
```

Terminal Local (3)

```
┌──(.venv)─(kali㉿kali)-[~/PycharmProjects/pythonProject]
└─$ python information-tool.py youtube.com
youtube.com

 {'Content-Type': 'text/html; charset=utf-8', 'X-Content-Type-Options': 'nosniff', 'Cache-Control': 'no-ca
che, no-store, max-age=0, must-revalidate', 'Pragma': 'no-cache', 'Expires': 'Mon, 01 Jan 1990 00:00:00 GM
T', 'Date': 'Mon, 20 May 2024 09:16:14 GMT', 'X-Frame-Options': 'SAMEORIGIN', 'Strict-Transport-Security':
 'max-age=31536000', 'Permissions-Policy': 'ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-ful
l-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-form-factor=*, ch-ua-platform=*, ch-ua-platform-vers
ion=*', 'Origin-Trial': 'AmhMBR6zCL2dDxpWeHfpP67BqwIknWnyMOXQQGfzYswFmJe+fgaI6XZgAzcxOrzNtP7hEDsOo1jdjFnVr
2IdxQ4AAAB4eyJvcmlnaW4iOiJodHwczovL3lvdXRlYmUuY29tOjQ0MyIsIm7lYXRlcmUiOiJXZWJWaWV3WFJlcXVlc3RlZFdpdGhEZXB
yZWNhdGlvbiIsIm V4cGlyeSI6MTc1ODA2NzE5OSwiaXNTdWJkb2lhaW4iOnRydWV9', 'Cross-Origin-Opener-Policy': 'same-or
igin-allow-popups; report-to="youtube_main"', 'Report-To': '{"group":"youtube_main","max_age":2592000,"end
points":[{"url":"https://csp.withgoogle.com/csp/report-to/youtube_main"}]}', 'P3P': 'CP="This is not a P3P
 policy! See http://support.google.com/accounts/answer/151657?hl=en-GB for more info."', 'Content-Encoding
': 'gzip', 'Server': 'ESF', 'X-XSS-Protection': '0', 'Set-Cookie': 'GPS=1; Domain=.youtube.com; Expires=Mo
n, 20-May-2024 09:46:14 GMT; Path=/; Secure; HttpOnly, YSC=2dDO1HATlKO; Domain=.youtube.com; Path=/; Secur
e; HttpOnly; SameSite=none, VISITOR_INFO1_LIVE=r3t94tBhEzE; Domain=.youtube.com; Expires=Sat, 16-Nov-2024
 09:16:14 GMT; Path=/; Secure; HttpOnly; SameSite=none, VISITOR_PRIVACY_METADATA=CgJJThIEGgAqTw%3D%3D; Doma
in=.youtube.com; Expires=Sat, 16-Nov-2024 09:16:14 GMT; Path=/; Secure; HttpOnly; SameSite=none', 'Alt-Svc
': 'h3=":443"; ma=2592000,h3-29=":443"; ma=2592000', 'Transfer-Encoding': 'chunked'}

*******************************************************

Scanning the IP address: 142.250.194.142 ==> youtube.com

Domain         : 142.250.194.142
Location       : 28.6519,77.2315
Region         : Delhi
City           : Delhi
Country        : IN
Postal         : 110001
Organisation   : AS15169 Google LLC
TimeZone       : Asia/Kolkata
Readme         : https://ipinfo.io/missingauth

*******************************************************
{'ip': '142.250.194.142', 'hostname': 'del12s05-in-f14.1e100.net', 'city': 'Delhi', 'region': 'Delhi', 'co
untry': 'IN', 'loc': '28.6519,77.2315', 'org': 'AS15169 Google LLC', 'postal': '110001', 'timezone': 'Asia
/Kolkata', 'readme': 'https://ipinfo.io/missingauth'}

┌──(.venv)─(kali㉿kali)-[~/PycharmProjects/pythonProject]
└─$
```

Here is the full view of program and compiled part.

****

Conclusion

This Python information gathering tool demonstrates a practical application for network reconnaissance and information retrieval from websites. By leveraging publicly available resources and libraries like `requests` and `socket`, the script automates the process of collecting valuable website details.

****