BABU BANARSI DAS UNIVERSITY

Identity and Access Management

Cyber security Tools

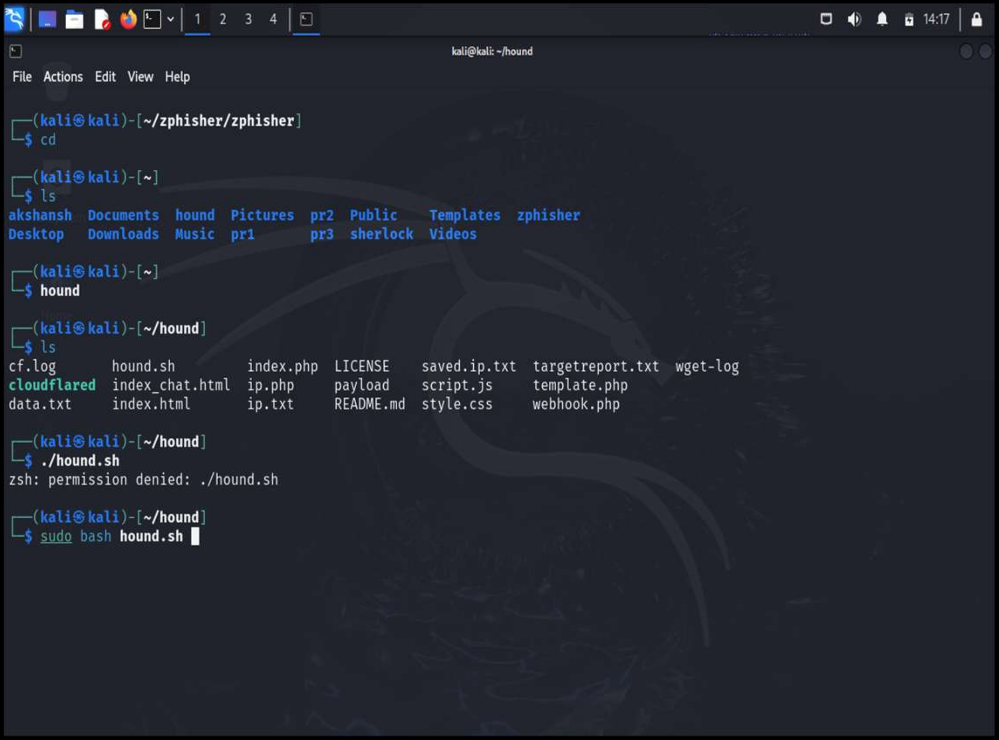
Submitted To:

Mr. Anand Kumar

Submitted By:

Akshansh Dwivedi

1240264016 (BCACS21)



```
┌──(kali㉿kali)-[~/zphisher/zphisher]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ ls
akshansh  Documents  hound  Pictures  pr2  Public    Templates  zphisher
Desktop   Downloads  Music  pr1       pr3  sherlock  Videos

┌──(kali㉿kali)-[~]
└─$ hound

┌──(kali㉿kali)-[~/hound]
└─$ ls
cf.log       hound.sh         index.php  LICENSE    saved.ip.txt  targetreport.txt  wget-log
cloudflared  index_chat.html  ip.php     payload    script.js     template.php
data.txt     index.html       ip.txt     README.md  style.css     webhook.php

┌──(kali㉿kali)-[~/hound]
└─$ ./hound.sh
zsh: permission denied: ./hound.sh

┌──(kali㉿kali)-[~/hound]
└─$ sudo bash hound.sh
```

1. Install Required Dependencies
Before using Hound, ensure your system has the necessary tools:
- Open a terminal and run:
sudo apt update
sudo apt install git php curl wget

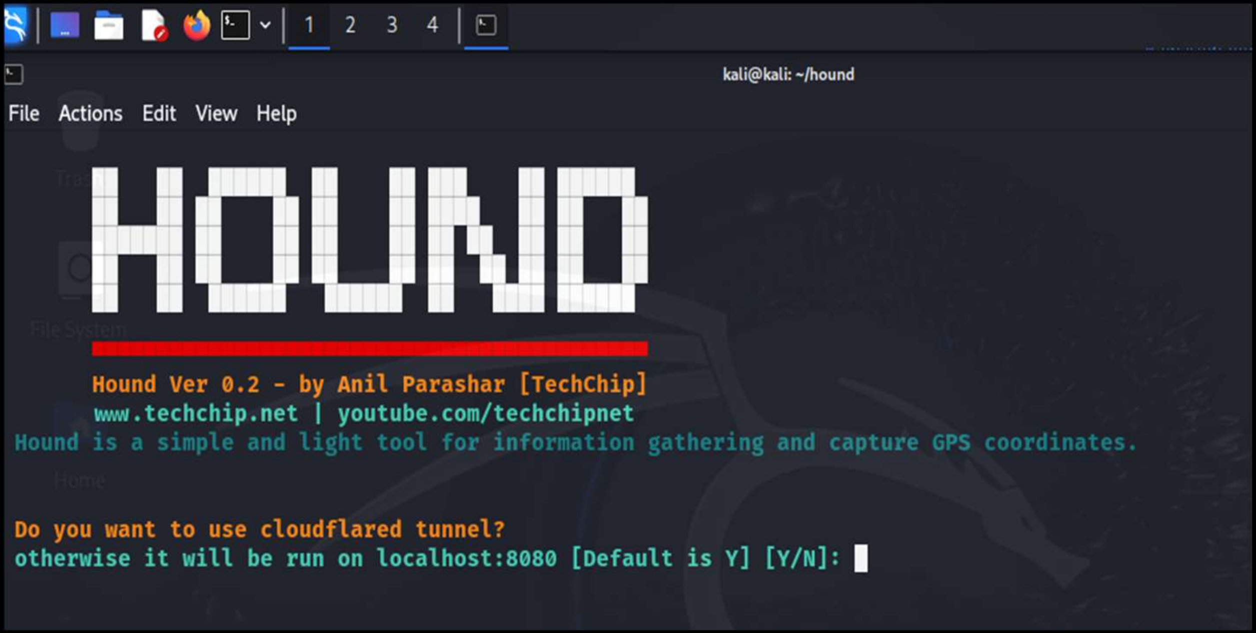
2. Clone the Hound Repository
- Use Git to download the tool:
git clone https://github.com/cybercrazy/Hound.gitcd Hound

3. Run the Setup Script
- Inside the Hound directory, execute:

- chmod +x hound.sh ./hound.sh
- This script sets up a Cloudflared tunnel and launches the PHP server.

4. Choose a Payload Type
- Hound offers multiple payloads for gathering information:
  - GPS location tracking
  - Device.
  - info
  - Browser fingerprinting
- Select the desired payload when prompted

HOUND



```
Hound Ver 0.2 - by Anil Parashar [TechChip]
www.techchip.net | youtube.com/techchipnet
Hound is a simple and light tool for information gathering and capture GPS coordinates.

Do you want to use cloudflared tunnel?
otherwise it will be run on localhost:8080 [Default is Y] [Y/N]:
```

- **Run the Setup Script**
- Inside the Hound directory, execute:
- chmod +x hound.sh
  ./hound.sh

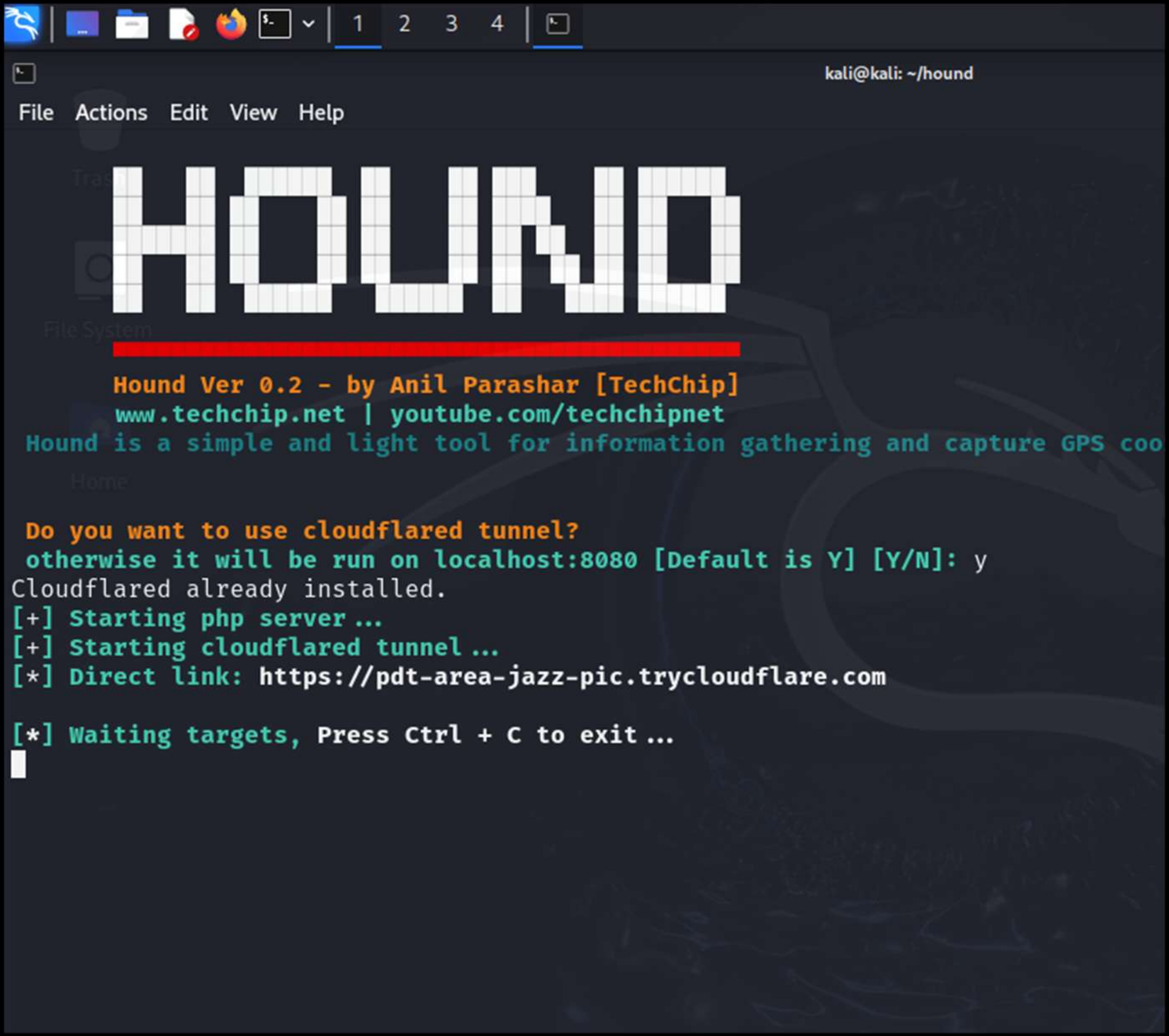
THIS SCRIPT SETS UP A CLOUDFLARED TUNNEL AND LAUNCHES THE PHP SERVER.

4. **Choose a Payload Type**

Hound offers multiple payloads for gathering information:

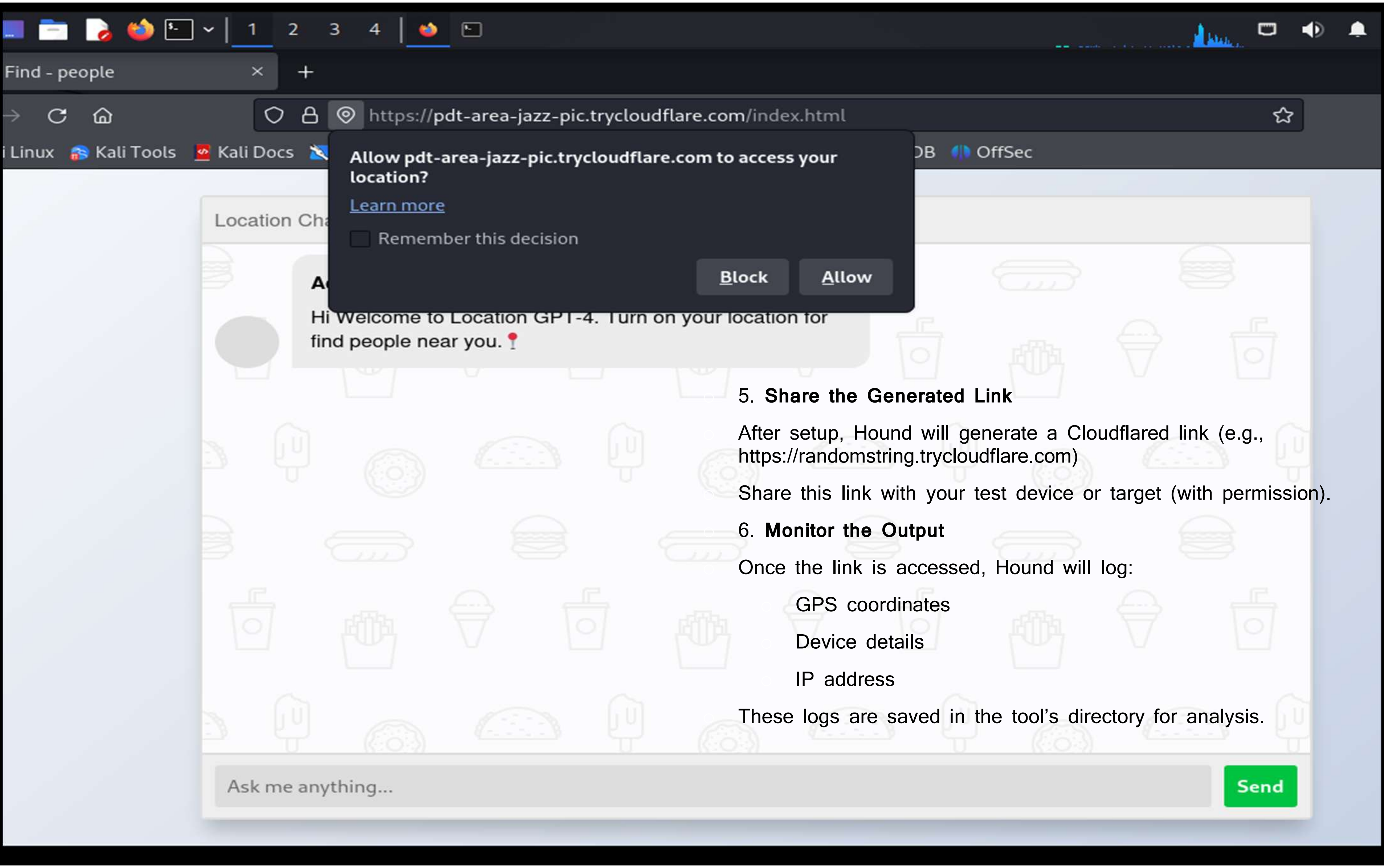
- GPS location tracking
- Device info
- Browser fingerprinting

Select the desired payload when prompted.



```
Hound Ver 0.2 - by Anil Parashar [TechChip]
www.techchip.net | youtube.com/techchipnet
Hound is a simple and light tool for information gathering and capture GPS coo

Do you want to use cloudflared tunnel?
otherwise it will be run on localhost:8080 [Default is Y] [Y/N]: y
Cloudflared already installed.
[+] Starting php server...
[+] Starting cloudflared tunnel...
[*] Direct link: https://pdt-area-jazz-pic.trycloudflare.com

[*] Waiting targets, Press Ctrl + C to exit...
```

Share the Generated Link



https://pdt-area-jazz-pic.trycloudflare.com/index.html

Allow pdt-area-jazz-pic.trycloudflare.com to access your location?

□ Remember this decision

Hi Welcome to Location GPT-4. Turn on your location for find people near you. 📍

Ask me anything...

5. **Share the Generated Link**

After setup, Hound will generate a Cloudflared link (e.g., https://randomstring.trycloudflare.com)

Share this link with your test device or target (with permission).

6. **Monitor the Output**

Once the link is accessed, Hound will log:

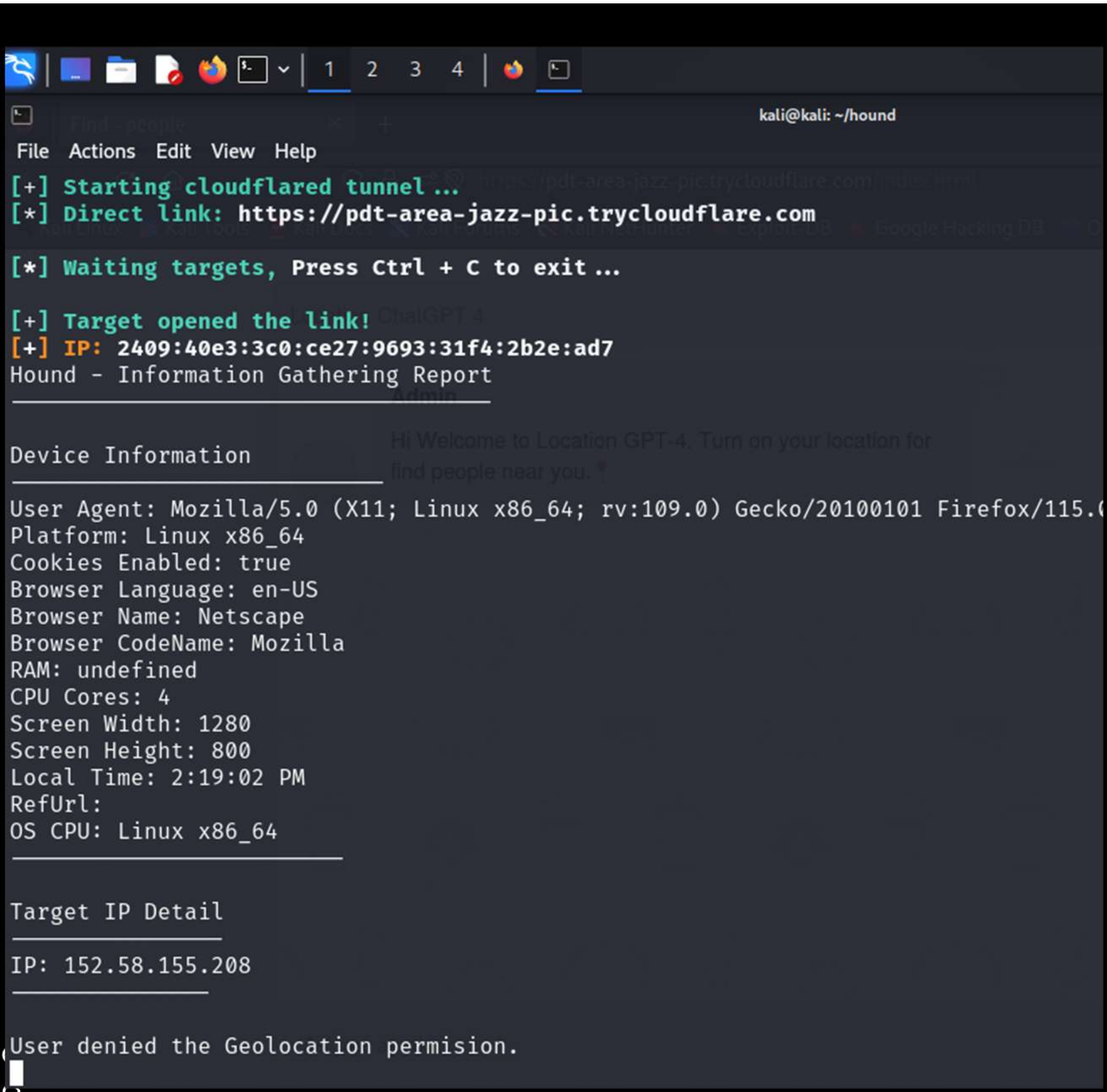
GPS coordinates

Device details

IP address

These logs are saved in the tool’s directory for analysis.

HOUND



```
[+] Starting cloudflared tunnel ...
[*] Direct link: https://pdt-area-jazz-pic.trycloudflare.com

[*] Waiting targets, Press Ctrl + C to exit ...

[+] Target opened the link!
[+] IP: 2409:40e3:3c0:ce27:9693:31f4:2b2e:ad7
Hound - Information Gathering Report
____________________________________

Device Information
____________________________

User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.
Platform: Linux x86_64
Cookies Enabled: true
Browser Language: en-US
Browser Name: Netscape
Browser CodeName: Mozilla
RAM: undefined
CPU Cores: 4
Screen Width: 1280
Screen Height: 800
Local Time: 2:19:02 PM
RefUrl:
OS CPU: Linux x86_64
_________________________

Target IP Detail
________________

IP: 152.58.155.208
_______________

User denied the Geolocation permision.
```

- GPS coordinates
- Device details
- IP address
- These logs are saved in the tool’s directory for analysis.

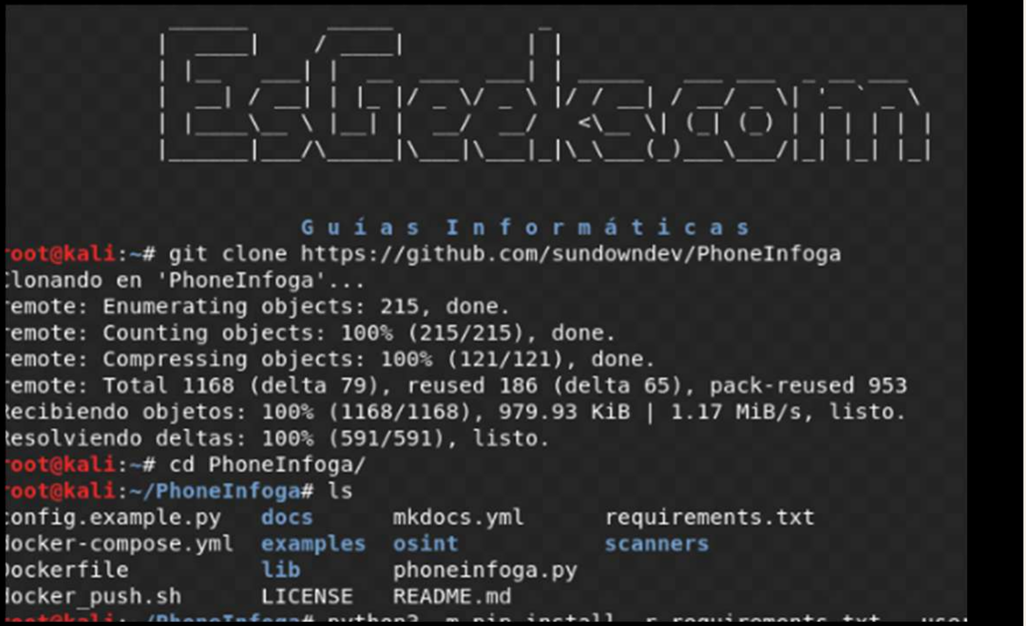
7. Analyze the Data

- Open the log files using any text editor or terminal:

- Use the data for learning how reconnaissance tools gather and present information.

We got the Desired results (HEHE! Let’s go boy)

HOUND



```
                  G u í a s   I n f o r m á t i c a s
root@kali:~# git clone https://github.com/sundowndev/PhoneInfoga
Clonando en 'PhoneInfoga'...
remote: Enumerating objects: 215, done.
remote: Counting objects: 100% (215/215), done.
remote: Compressing objects: 100% (121/121), done.
remote: Total 1168 (delta 79), reused 186 (delta 65), pack-reused 953
Recibiendo objetos: 100% (1168/1168), 979.93 KiB | 1.17 MiB/s, listo.
Resolviendo deltas: 100% (591/591), listo.
root@kali:~# cd PhoneInfoga/
root@kali:~/PhoneInfoga# ls
config.example.py   docs      mkdocs.yml      requirements.txt
docker-compose.yml  examples  osint           scanners
Dockerfile          lib       phoneinfoga.py
docker_push.sh      LICENSE   README.md
root@kali:~/PhoneInfoga# python3 -m pip install -r requirements.txt --use
```

Phoneinfoga

1.Open your terminal and run:
sudo apt update sudo apt install git python3 python3-pip

2. Clone the PhoneInfoga Repository
git clone https://github.com/sundowndev/phoneinfoga.git cd phoneinfoga

3. Install Python Requirements
pip3 install -r requirements.txt

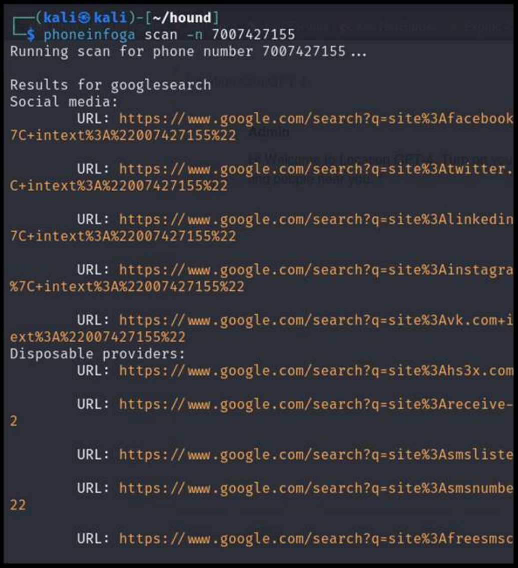
4. Run PhoneInfoga
You can now launch the tool:
python3 phoneinfoga.py -n +911234567890
Replace +911234567890 with the phone number you want to analyze (with permission).

5. Use Advanced Scanning (Optional)
To enable more detailed scans:
Configure external APIs in the config.example.json file.
Rename it to config.json and add your API keys (e.g., Numverify, Twilio).

6. View Results
The tool will display:
Country and region
Carrier information
Line type (mobile, landline, VoIP)
Possible social media or breach links (if configured)

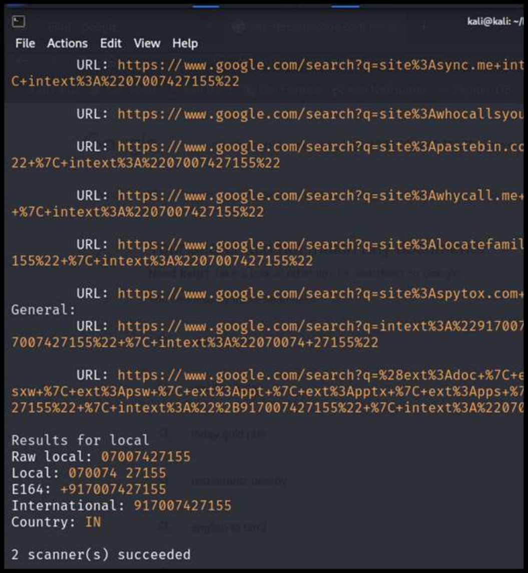
METHODOLOGY AND RESULTS

PHONEINFOGA



```
┌──(kali㉿kali)-[~/hound]
└─$ phoneinfoga scan -n 7007427155
Running scan for phone number 7007427155 ...

Results for googlesearch
Social media:
        URL: https://www.google.com/search?q=site%3Afacebook
7C+intext%3A%22007427155%22

        URL: https://www.google.com/search?q=site%3Atwitter.
C+intext%3A%22007427155%22

        URL: https://www.google.com/search?q=site%3Alinkedin
7C+intext%3A%22007427155%22

        URL: https://www.google.com/search?q=site%3Ainstagra
%7C+intext%3A%22007427155%22

        URL: https://www.google.com/search?q=site%3Avk.com+i
ext%3A%22007427155%22
Disposable providers:
        URL: https://www.google.com/search?q=site%3Ahs3x.com

        URL: https://www.google.com/search?q=site%3Areceive-
2

        URL: https://www.google.com/search?q=site%3Asmsliste

        URL: https://www.google.com/search?q=site%3Asmsnumbe
22

        URL: https://www.google.com/search?q=site%3Afreesmsc
```

Give the command and wait for few seconds it will provide you with the google dorks on the provided number for extreme useful information.



```
        URL: https://www.google.com/search?q=site%3Async.me+int
C+intext%3A%2207007427155%22

        URL: https://www.google.com/search?q=site%3Awhocallsyou

        URL: https://www.google.com/search?q=site%3Apastebin.co
22+%7C+intext%3A%2207007427155%22

        URL: https://www.google.com/search?q=site%3Awhycall.me+
+%7C+intext%3A%2207007427155%22

        URL: https://www.google.com/search?q=site%3Alocatefamil
155%22+%7C+intext%3A%2207007427155%22

        URL: https://www.google.com/search?q=site%3Aspytox.com+
General:
        URL: https://www.google.com/search?q=intext%3A%22917007
7007427155%22+%7C+intext%3A%22070074+27155%22

        URL: https://www.google.com/search?q=%28ext%3Adoc+%7C+e
sxw+%7C+ext%3Apsw+%7C+ext%3Appt+%7C+ext%3Apptx+%7C+ext%3Apps+%7
27155%22+%7C+intext%3A%22%2B917007427155%22+%7C+intext%3A%22070

Results for local
Raw local: 07007427155
Local: 070074 27155
E164: +917007427155
International: 917007427155
Country: IN

2 scanner(s) succeeded
```

Here are the results the country and the dorking targets

🧪 Student Use Cases

- Learn OSINT techniques for phone-based reconnaissance.
- Understand metadata associated with mobile numbers.
- Practice ethical scanning in lab environments or with dummy/test numbers.

🔐 Ethical Reminder

Always use PhoneInfoga:

- On your own numbers
- In lab simulations
- With explicit permission

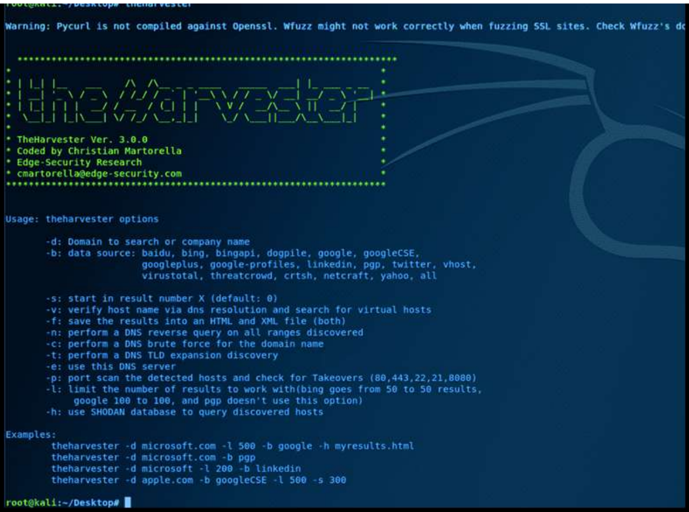
Unauthorized use may violate privacy laws and ethical standards.

OTHER TOOLS USED

KALI LINUX

Tools used: -

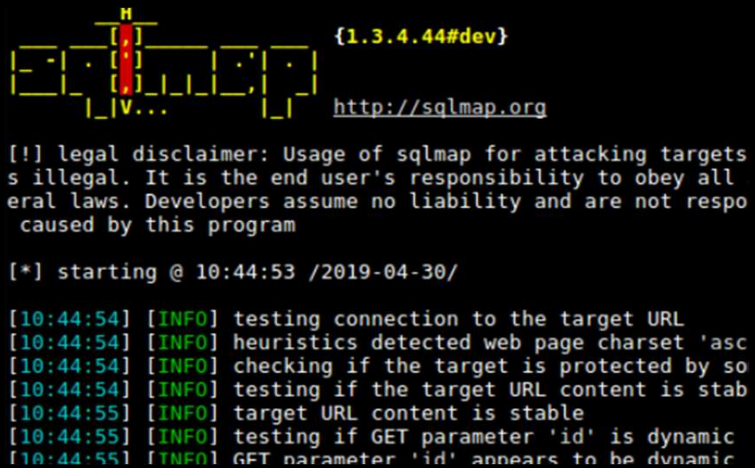
Theharvester, hydra, nmap, wireshark, autopsy, ngork, phoneinfoga, sqlmap, dnsenum, burpsuite, volatility, etc.



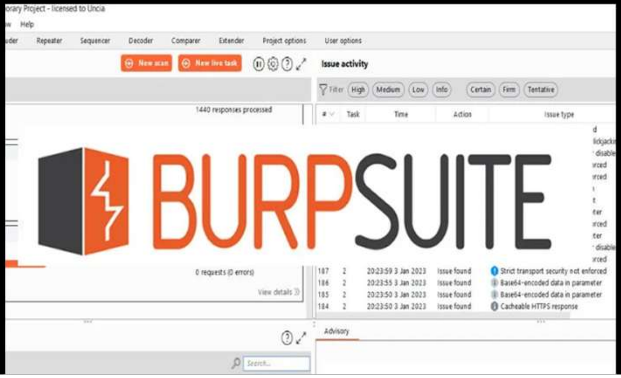
```
root@kali:~/Desktop# theharvester

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's dc

 *******************************************************************
 *                                                                 *
 *                                                                 *
 * TheHarvester Ver. 3.0.0                                         *
 * Coded by Christian Martorella                                   *
 * Edge-Security Research                                          *
 * cmartorella@edge-security.com                                   *
 *******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
                        googleplus, google-profiles, linkedin, pgp, twitter, vhost,
                        virustotal, threatcrowd, crtsh, netcraft, yahoo, all

       -s: start in result number X (default: 0)
       -v: verify host name via dns resolution and search for virtual hosts
       -f: save the results into an HTML and XML file (both)
       -n: perform a DNS reverse query on all ranges discovered
       -c: perform a DNS brute force for the domain name
       -t: perform a DNS TLD expansion discovery
       -e: use this DNS server
       -p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
       -l: limit the number of results to work with(bing goes from 50 to 50 results,
            google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
        theharvester -d microsoft.com -l 500 -b google -h myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300

root@kali:~/Desktop#
```

```
ra -h"
019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal pu

[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-

ore a previous aborted/crashed session
re an existing restore file (don't wait 10 seconds)
orm an SSL connect
he service is on a different default port, define it here
 FILE  login with LOGIN name, or load several logins from FILE
 FILE  try password PASS, or load several passwords from FILE
RSET  password bruteforce generation, type "-x -h" to get help
ble use of symbols in bruteforce, see above
"n" null password, "s" login as pass and/or "r" reversed login
 around users, not passwords (effective! implied with -x)
n separated "login:pass" format, instead of -L/-P options
 of servers to attack, one entry per line, ':' to specify port
e found login/password pairs to FILE instead of stdout
ify the format for the -o FILE: text(default), json, jsonv1
 when a login/pass pair is found (-M: -f per host, -F global)
TASKS number of connects in parallel per target (default: 16)
TASKS connects in parallel overall (for -M, default: 64)
wait time for a response (32) / between connects per thread (0)
 time per login attempt over all threads (enforces -t 1)
IPv4 (default) / IPv6 addresses (put always in [] also in -M)
verbose mode / show login+pass for each attempt / debug mode
old SSL v2 and v3
ot print messages about connection errors
ice module usage details
 command line options (COMPLETE HELP)
target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service to crack (see below for supported protocols)
 service modules support additional input (-U for module help)

es: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-
istener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-30

 to guess/crack valid login/password pairs. Licensed under AGPL
 version is always available at https://github.com/vanhauser-thc/thc-hydra
itary or secret service organizations, or for illegal purposes.
ere not compiled in: afp ncp oracle sapr3).

HTTP or HYDRA_PROXY environment variables for a proxy setup.
DRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect://)
DRA_PROXY=connect_and_socks_proxylist.txt  (up to 64 entries)
DRA_PROXY_HTTP=http://login:pass@proxy:8080
DRA_PROXY_HTTP=proxylist.txt  (up to 64 entries)


-P passlist.txt ftp://192.168.0.1
ist.txt -p defaultpw imap://192.168.0.1/PLAIN
lts.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
 -p password ftp://[192.168.0.0/24]/
s.txt -P pws.txt -M targets.txt ssh
```

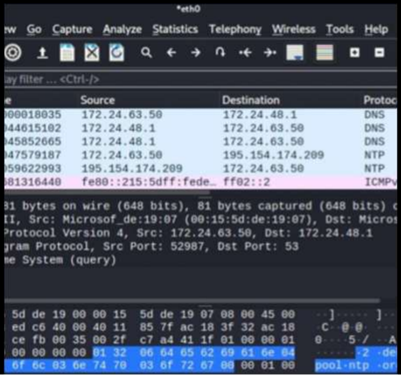
```
ome/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults
p 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
port for scanme.nmap.org (45.33.32.156)
0.21s latency).
ses for scanme.nmap.org (not          2600:3c01::f03c:91ff:fe1
87 closed ports
ATE    SERVICE
en     ssh                                   ntu2.13 (Ubunt

ltered smtp
en     http
ltered msrpc
ltered netbios
ltered microsoft-ds
ltered http-rpc-epmap
ltered instl_bootc
ltered krb524
ltered vnc-http
ltered vnc
en     nping-echo
en     tcpwrapped
: OS: Linux; CPE: cp

ction performed. Please report any incorrect results at https:/

 IP address (1 host up) scanned in 39.35 seconds
```



```
                          {1.3.4.44#dev}

                          http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets
s illegal. It is the end user's responsibility to obey all
eral laws. Developers assume no liability and are not respo
 caused by this program

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'asc
[10:44:54] [INFO] checking if the target is protected by so
[10:44:54] [INFO] testing if the target URL content is stab
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
```



#	Task	Time	Action	Issue type
187	2	20:23:59 3 Jan 2023	Issue found	Strict transport security not enforced
186	2	20:23:55 3 Jan 2023	Issue found	Base64-encoded data in parameter
185	2	20:23:50 3 Jan 2023	Issue found	Base64-encoded data in parameter
184	2	20:23:50 3 Jan 2023	Issue found	Cacheable HTTPS response



e	Source	Destination	Protoc
000018035	172.24.63.50	172.24.48.1	DNS
044615102	172.24.48.1	172.24.63.50	DNS
045852665	172.24.48.1	172.24.63.50	DNS
047579187	172.24.63.50	195.154.174.209	NTP
059622993	195.154.174.209	172.24.63.50	NTP
681316440	fe80::215:5dff:fede…	ff02::2	ICMPv

```
81 bytes on wire (648 bits), 81 bytes captured (648 bits) c
II, Src: Microsof_de:19:07 (00:15:5d:de:19:07), Dst: Micros
Protocol Version 4, Src: 172.24.63.50, Dst: 172.24.48.1
gram Protocol, Src Port: 52987, Dst Port: 53
me System (query)

 5d de 19 00 00 15  5d de 19 07 08 00 45 00   ··]·····]··
 ed c6 40 00 40 11  85 7f ac 18 3f 32 ac 18   ·C··@·@····
 ce fb 00 35 00 2f  c7 a4 41 1f 01 00 00 01   0···5·/··A
 00 00 00 00 01 32  06 64 65 62 69 61 6e 04   ······2·de
 6f 6c 03 6e 74 70  03 6f 72 67 00 00 01 00   pool·ntp·or
```