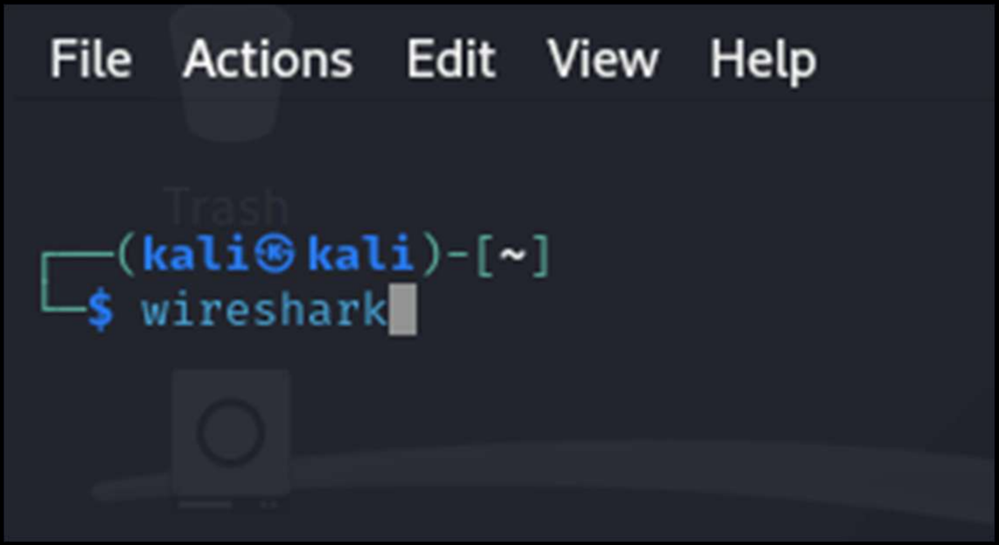


```
┌──(kali㉿kali)-[~]
└─$ wireshark
```

To use Wireshark effectively, follow these steps: install the tool, select the correct network interface, start capturing packets, apply filters, and analyze the data. Here's a detailed breakdown tailored for your cybersecurity workflow:

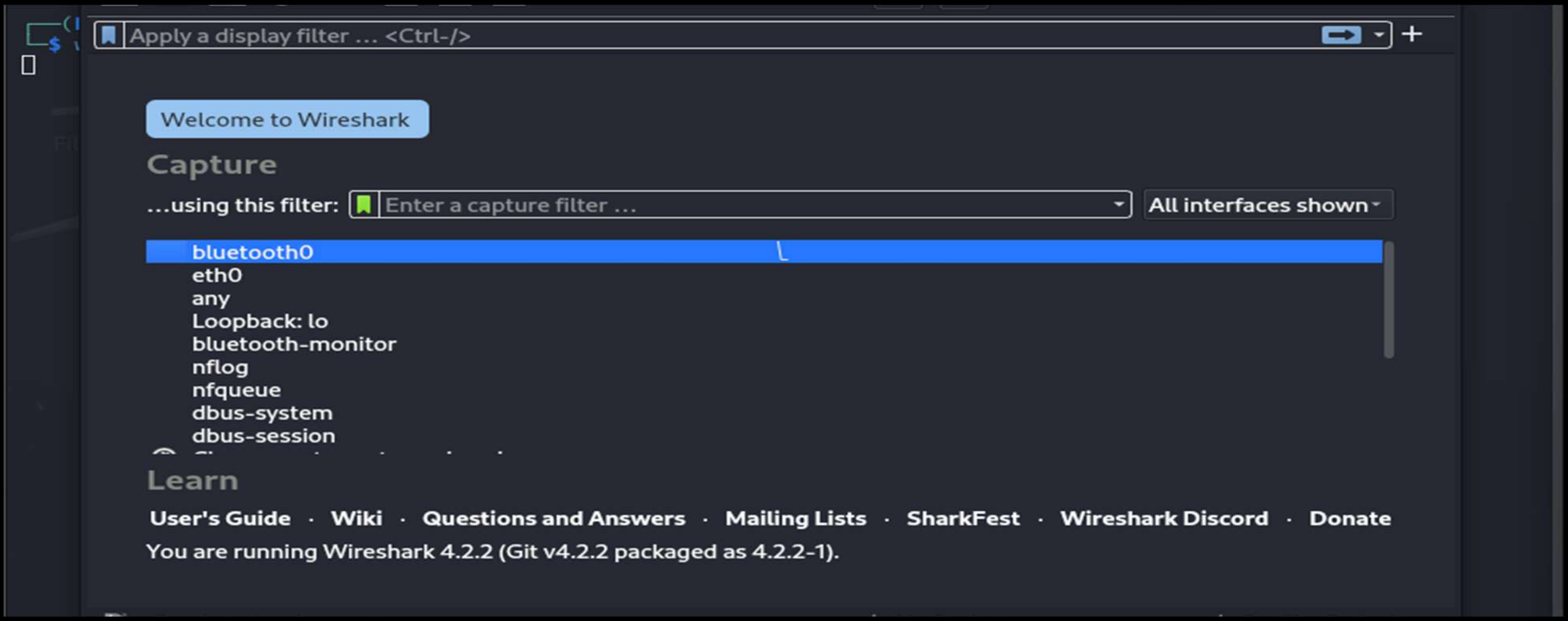
Step-by-Step Guide to Using Wireshark

1. **Install Wireshark**
Download from the official Wireshark website.
Choose the correct installer for your OS (Windows, Linux, macOS).
During installation, allow WinPcap or Npcap (required for packet capture on Windows).

2. **Launch Wireshark and Select Interface**
Open Wireshark and you'll see a list of available network interfaces.
Choose the one actively transmitting data (often your Ethernet or Wi-Fi adapter).

Click the blue shark fin icon to start capturing packets.

3. **Start Capturing Packets**
Once capture begins, Wireshark displays real-time packet data.
You'll see columns like *Time*, *Source*, *Destination*, *Protocol*, and *Info*.
Let it run for a few seconds or minutes depending on your analysis needs.



Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

```
bluetooth0
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
```

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1).

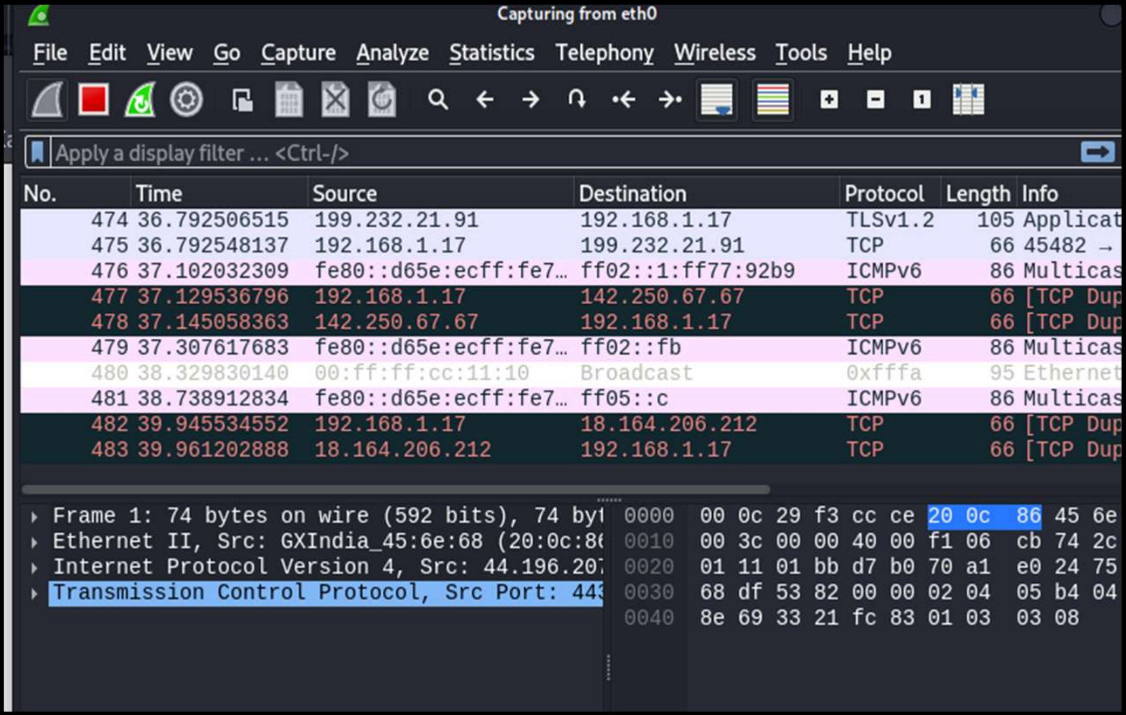
- •Open Wireshark and you'll see a list of available network interfaces.
- •Choose the one actively transmitting data (often your Ethernet or Wi-Fi adapter).
- •Click the blue shark fin icon to start capturing packets

3. Start Capturing Packets

- Once capture begins, Wireshark displays real-time packet data.
- You’ll see columns like Time, Source, Destination, Protocol, and Info.
- Let it run for a few seconds or minutes depending on your analysis needs.

4. Apply Capture or Display Filters

- Capture filters (set before starting): limit what gets recorded (e.g.,).
- Display filters (set after capture): narrow down what you see (e.g., ,).
- Use the filter bar at the top to enter expressions.



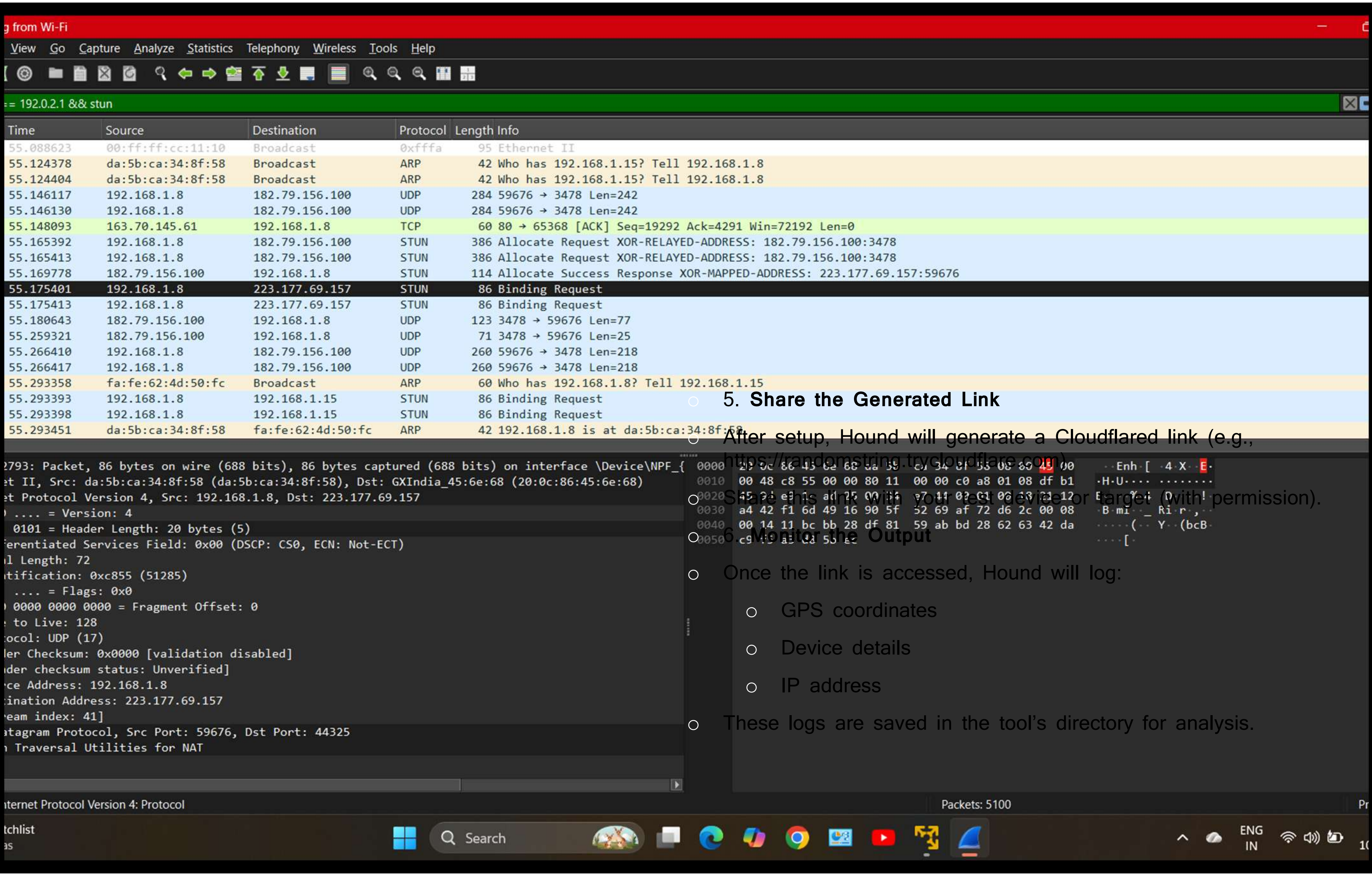
No.	Time	Source	Destination	Protocol	Length	Info
474	36.792506515	199.232.21.91	192.168.1.17	TLSv1.2	105	Applicat
475	36.792548137	192.168.1.17	199.232.21.91	TCP	66	45482 →
476	37.102032309	fe80::d65e:ecff:fe7…	ff02::1:ff77:92b9	ICMPv6	86	Multicas
477	37.129536796	192.168.1.17	142.250.67.67	TCP	66	[TCP Dup
478	37.145058363	142.250.67.67	192.168.1.17	TCP	66	[TCP Dup
479	37.307617683	fe80::d65e:ecff:fe7…	ff02::fb	ICMPv6	86	Multicas
480	38.329830140	00:ff:ff:cc:11:10	Broadcast	0xfffa	95	Ethernet
481	38.738912834	fe80::d65e:ecff:fe7…	ff05::c	ICMPv6	86	Multicas
482	39.945534552	192.168.1.17	18.164.206.212	TCP	66	[TCP Dup
483	39.961202888	18.164.206.212	192.168.1.17	TCP	66	[TCP Dup

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 byt      0000   00 0c 29 f3 cc ce 20 0c  86 45 6e
▸ Ethernet II, Src: GXIndia_45:6e:68 (20:0c:86      0010   00 3c 00 00 40 00 f1 06  cb 74 2c
▸ Internet Protocol Version 4, Src: 44.196.20       0020   01 11 01 bb d7 b0 70 a1  e0 24 75
▸ Transmission Control Protocol, Src Port: 44       0030   68 df 53 82 00 00 02 04  05 b4 04
                                                    0040   8e 69 33 21 fc 83 01 03  03 08
```

5. **Analyze Packets**

- Click on any packet to expand its details.
- You can inspect layers like Ethernet, IP, TCP/UDP, and application protocols (e.g., HTTP, DNS).
- Right-click a packet to follow TCP streams or export data.

HOUND



```
:= 192.0.2.1 && stun

Time       Source             Destination       Protocol Length Info
55.088623  00:ff:ff:cc:11:10  Broadcast         0xfffa     95 Ethernet II
55.124378  da:5b:ca:34:8f:58  Broadcast         ARP        42 Who has 192.168.1.15? Tell 192.168.1.8
55.124404  da:5b:ca:34:8f:58  Broadcast         ARP        42 Who has 192.168.1.15? Tell 192.168.1.8
55.146117  192.168.1.8        182.79.156.100    UDP       284 59676 → 3478 Len=242
55.146130  192.168.1.8        182.79.156.100    UDP       284 59676 → 3478 Len=242
55.148093  163.70.145.61      192.168.1.8       TCP        60 80 → 65368 [ACK] Seq=19292 Ack=4291 Win=72192 Len=0
55.165392  192.168.1.8        182.79.156.100    STUN      386 Allocate Request XOR-RELAYED-ADDRESS: 182.79.156.100:3478
55.165413  192.168.1.8        182.79.156.100    STUN      386 Allocate Request XOR-RELAYED-ADDRESS: 182.79.156.100:3478
55.169778  182.79.156.100     192.168.1.8       STUN      114 Allocate Success Response XOR-MAPPED-ADDRESS: 223.177.69.157:59676
55.175401  192.168.1.8        223.177.69.157    STUN       86 Binding Request
55.175413  192.168.1.8        223.177.69.157    STUN       86 Binding Request
55.180643  182.79.156.100     192.168.1.8       UDP       123 3478 → 59676 Len=77
55.259321  182.79.156.100     192.168.1.8       UDP        71 3478 → 59676 Len=25
55.266410  192.168.1.8        182.79.156.100    UDP       260 59676 → 3478 Len=218
55.266417  192.168.1.8        182.79.156.100    UDP       260 59676 → 3478 Len=218
55.293358  fa:fe:62:4d:50:fc  Broadcast         ARP        60 Who has 192.168.1.8? Tell 192.168.1.15
55.293393  192.168.1.8        192.168.1.15      STUN       86 Binding Request
55.293398  192.168.1.8        192.168.1.15      STUN       86 Binding Request
55.293451  da:5b:ca:34:8f:58  fa:fe:62:4d:50:fc ARP        42 192.168.1.8 is at da:5b:ca:34:8f:58

2793: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{
et II, Src: da:5b:ca:34:8f:58 (da:5b:ca:34:8f:58), Dst: GXIndia_45:6e:68 (20:0c:86:45:6e:68)
et Protocol Version 4, Src: 192.168.1.8, Dst: 223.177.69.157
) .... = Version: 4
 0101 = Header Length: 20 bytes (5)
ferentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
al Length: 72
ntification: 0xc855 (51285)
 .... = Flags: 0x0
) 0000 0000 0000 = Fragment Offset: 0
e to Live: 128
tocol: UDP (17)
der Checksum: 0x0000 [validation disabled]
ader checksum status: Unverified]
rce Address: 192.168.1.8
tination Address: 223.177.69.157
ream index: 41]
atagram Protocol, Src Port: 59676, Dst Port: 44325
n Traversal Utilities for NAT

0000  20 0c 86 45 6e 68 da 5b  ca 34 8f 58 08 00 45 00   ··Enh·[ ·4·X··E·
0010  00 48 c8 55 00 00 80 11  00 00 c0 a8 01 08 df b1   ·H·U···· ········
0020  [illegible]                                        [illegible]
0030  a4 42 f1 6d 49 16 90 5f  52 69 af 72 d6 2c 00 08   ·B·mI··_ Ri·r·,··
0040  00 14 11 bc bb 28 df 81  59 ab bd 28 62 63 42 da   ·····(·· Y··(bcB·
0050  c9 [illegible] a3 c8 5b ee                         ····[·

Internet Protocol Version 4: Protocol        Packets: 5100
```

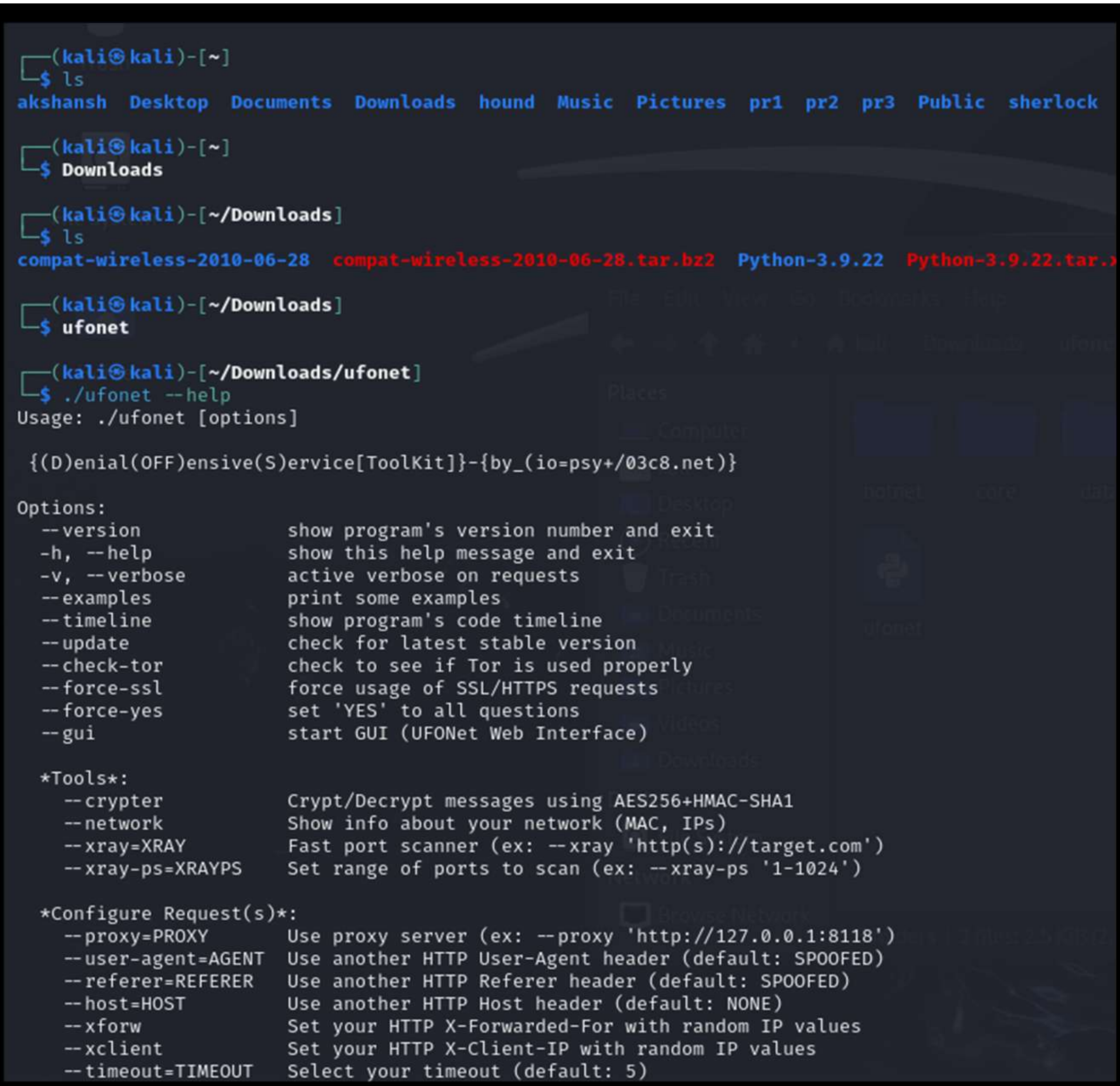
5. **Share the Generated Link**

- 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



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

┌──(kali㉿kali)-[~]
└─$ Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
compat-wireless-2010-06-28  compat-wireless-2010-06-28.tar.bz2  Python-3.9.22  Python-3.9.22.tar.x

┌──(kali㉿kali)-[~/Downloads]
└─$ ufonet

┌──(kali㉿kali)-[~/Downloads/ufonet]
└─$ ./ufonet --help
Usage: ./ufonet [options]

 {(D)enial(OFF)ensive(S)ervice[ToolKit]}-{by_(io=psy+/03c8.net)}

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -v, --verbose         active verbose on requests
  --examples            print some examples
  --timeline            show program's code timeline
  --update              check for latest stable version
  --check-tor           check to see if Tor is used properly
  --force-ssl           force usage of SSL/HTTPS requests
  --force-yes           set 'YES' to all questions
  --gui                 start GUI (UFONet Web Interface)

  *Tools*:
    --crypter           Crypt/Decrypt messages using AES256+HMAC-SHA1
    --network           Show info about your network (MAC, IPs)
    --xray=XRAY         Fast port scanner (ex: --xray 'http(s)://target.com')
    --xray-ps=XRAYPS    Set range of ports to scan (ex: --xray-ps '1-1024')

  *Configure Request(s)*:
    --proxy=PROXY       Use proxy server (ex: --proxy 'http://127.0.0.1:8118')
    --user-agent=AGENT  Use another HTTP User-Agent header (default: SPOOFED)
    --referer=REFERER   Use another HTTP Referer header (default: SPOOFED)
    --host=HOST         Use another HTTP Host header (default: NONE)
    --xforw             Set your HTTP X-Forwarded-For with random IP values
    --xclient           Set your HTTP X-Client-IP with random IP values
    --timeout=TIMEOUT   Select your timeout (default: 5)
```

Ethical DoS Simulation Lab with UFONet

✅ What You'll Need

Kali Linux (host or VM)

UFONet installed

Local web server (e.g., Apache or Flask app)

Isolated network or VM environment

🛠️ Setup Steps

Install UFONet

git clone https://github.com/epsylon/ufonet.git cd ufonet python3 ufonet --help

Set Up a Test Web Server Example using Python Flask:

pip3 install flask echo "from flask import Flask; app = Flask(__name__); @app.route('/') def home(): return 'Test Server'; app.run(host='0.0.0.0', port=8080)" > test_server.py python3 test_server.py

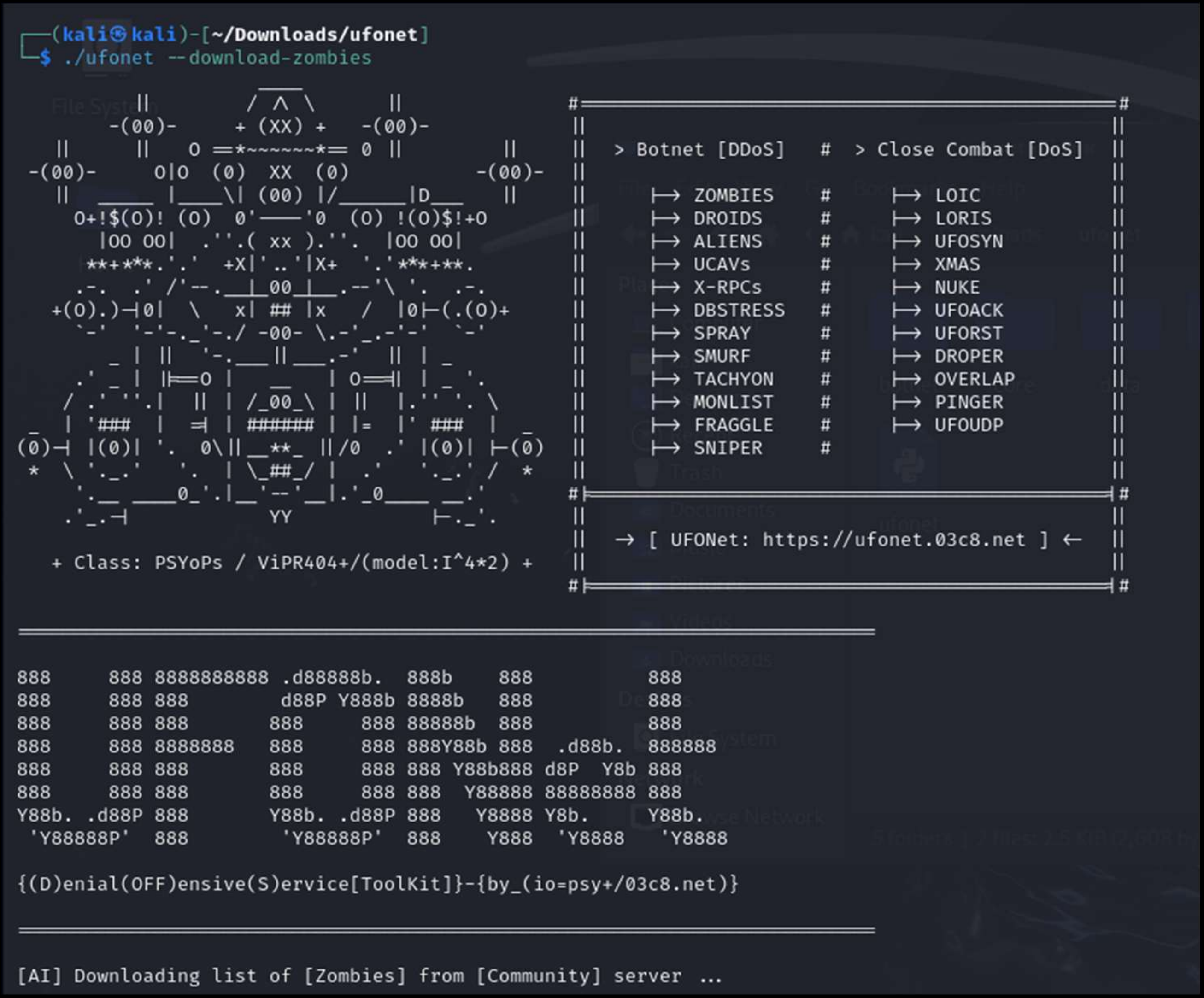
□□Download and Test Zombies

python3 ufonet --download-zombies python3 ufonet --test-zombies

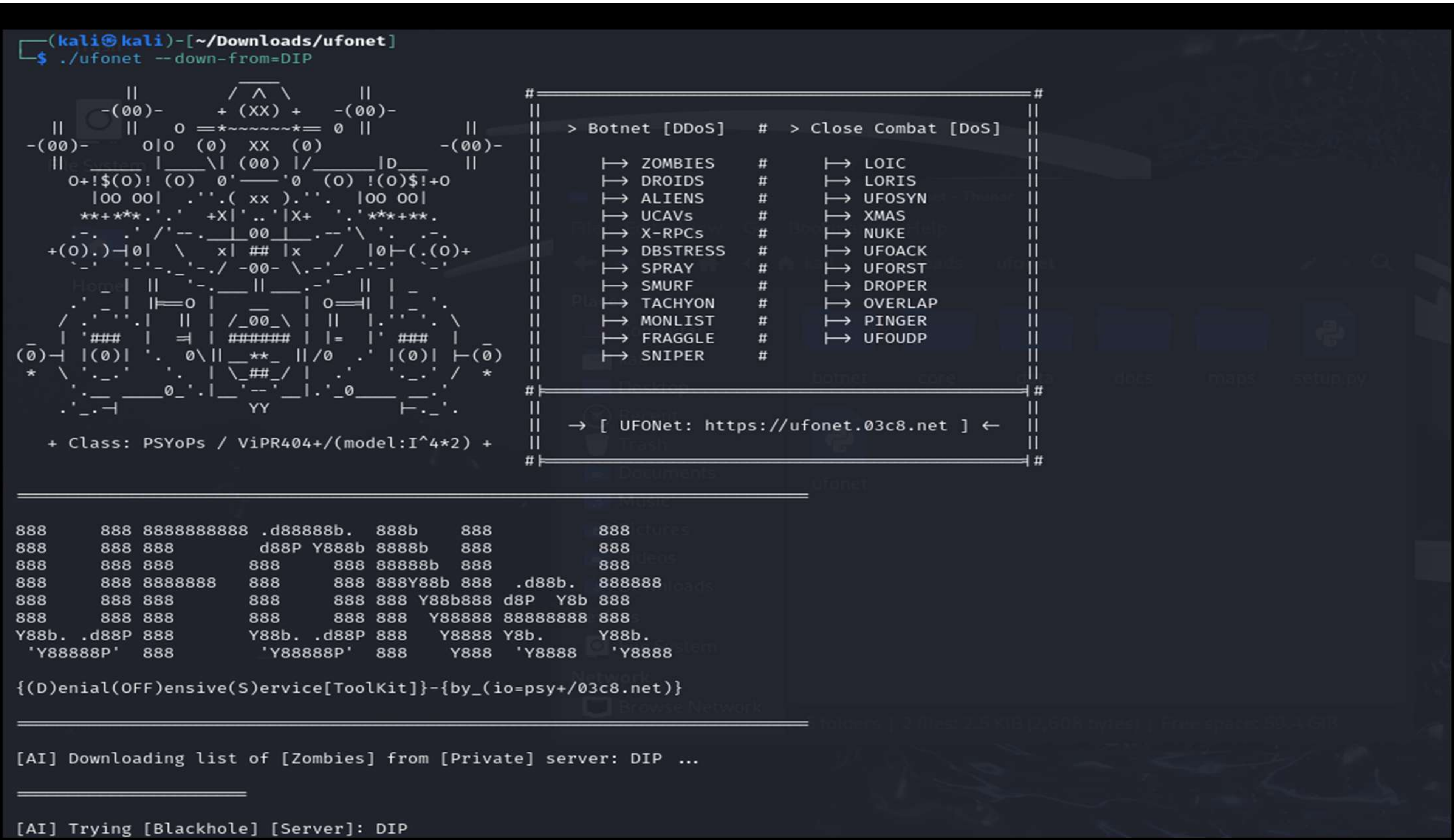
Simulate Attack on Localhost

python3 ufonet --attack --target http://127.0.0.1:8080

HOUND



```
┌──(kali㉿kali)-[~/Downloads/ufonet]
└─$ ./ufonet --download-zombies

                     ____
           ||       / ^ \        ||              #================================================#
        -(00)-     + (XX) +   -(00)-             ||                                              ||
   ||      ||   0 ==*~~~~~~~*== 0 ||        ||   ||   > Botnet [DDoS]    #  > Close Combat [DoS]  ||
 -(00)-      O|O  (0)  XX  (0)           -(00)-  ||                                              ||
   ||   ______ |____\| (00) |/______|D___   ||   ||      ⟼ ZOMBIES      #     ⟼ LOIC            ||
     O+!$(O)! (O)  0'———'0  (O) !(O)$!+O         ||      ⟼ DROIDS       #     ⟼ LORIS           ||
       |OO OO|  .''.( xx ).''.  |OO OO|          ||      ⟼ ALIENS       #     ⟼ UFOSYN          ||
      **+**.'.'  +X|'..'|X+  '.'**+**.           ||      ⟼ UCAVs        #     ⟼ XMAS            ||
     .-.  .' /'--.__|_00_|__.--'\ '.  .-.        ||      ⟼ X-RPCs       #     ⟼ NUKE            ||
   +(O).)⊣|0|  \    x| ## |x   /  |0⊢(.(O)+      ||      ⟼ DBSTRESS     #     ⟼ UFOACK          ||
     `-'  '-'-._'-./ -00- \.-'_.-'-'  `-'        ||      ⟼ SPRAY        #     ⟼ UFORST          ||
        _ | ||  '-.___||___.-'  || | _           ||      ⟼ SMURF        #     ⟼ DROPER          ||
     .' _ | ||==0 |   __   | O==|| | _ '.        ||      ⟼ TACHYON      #     ⟼ OVERLAP         ||
    / .'''.|  || | /_00_\ | ||  |.''''. \        ||      ⟼ MONLIST      #     ⟼ PINGER          ||
 _  | '###  |  =| | ###### | |=  |' ###  |  _    ||      ⟼ FRAGGLE      #     ⟼ UFOUDP          ||
(0)⊣ |(0)| '.  0\||__**_ ||/0  .' |(0)| ⊢(0)     ||      ⟼ SNIPER       #                       ||
 *  \ '._.'  '.  | \_##_/ |  .'  '._.' /  *      ||                                              ||
     '.__ _____0_'.|__'--'__|.'_0_____ __.'      #⊨==============================================⊨#
    .'_.⊣          YY          ⊢._'.             ||                                              ||
                                                 ||   → [ UFONet: https://ufonet.03c8.net ] ←    ||
   + Class: PSYoPs / ViPR404+/(model:I^4*2) +    ||                                              ||
                                                 #⊨==============================================⊨#

══════════════════════════════════════════════════════════════════════════

888     888 8888888888 .d88888b.  888b    888          888
888     888 888       d88P Y888b 8888b   888          888
888     888 888      888     888 88888b  888          888
888     888 8888888  888     888 888Y88b 888  .d88b.  888888
888     888 888      888     888 888 Y88b888 d8P  Y8b 888
888     888 888      888     888 888  Y88888 88888888 888
Y88b. .d88P 888      Y88b. .d88P 888   Y8888 Y8b.     Y88b.
 'Y88888P'  888       'Y88888P'  888    Y888  'Y8888   'Y8888

{(D)enial(OFF)ensive(S)ervice[ToolKit]}-{by_(io=psy+/03c8.net)}

══════════════════════════════════════════════════════════════════════════

[AI] Downloading list of [Zombies] from [Community] server ...
```



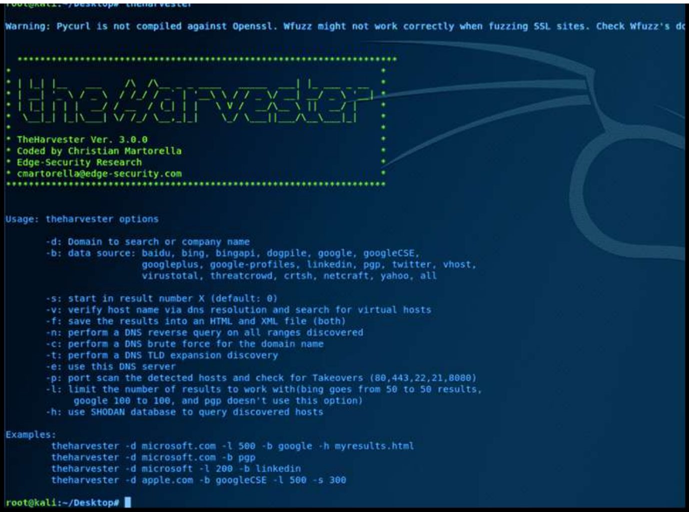
```
┌──(kali㉿kali)-[~/Downloads/ufonet]
└─$ ./ufonet --down-from=DIP

                     ____
           ||        /  ^ \       ||              #════════════════════════════════════════════════#
        -(00)-     + (XX) +   -(00)-              ||                                              ||
    ||     ||  O ══*~~~~~~~*══ 0 ||        ||     ||  > Botnet [DDoS]   #  > Close Combat [DoS]   ||
 -(00)-    O|O  (0)  XX  (0)           -(00)-     ||                                              ||
    ||  _____|_____\| (00) |/_______|D___   ||    ||     ├─→ ZOMBIES    #     ├─→ LOIC            ||
     O+!$(O)! (O)  0'────'0  (O) !(O)$!+O         ||     ├─→ DROIDS     #     ├─→ LORIS           ||
       |OO OO|  .''.( xx ).''.  |OO OO|           ||     ├─→ ALIENS     #     ├─→ UFOSYN          ||
      **+***.'.'  +X|'..'|X+  '.'***+**.          ||     ├─→ UCAVs      #     ├─→ XMAS            ||
     .-.  .' /'--.__|_00_|___.--'\ '.  .-.        ||     ├─→ X-RPCs     #     ├─→ NUKE            ||
   +(O).)─┤0|  \    x| ## |x   /  |0├─(.(O)+      ||     ├─→ DBSTRESS   #     ├─→ UFOACK          ||
     `-'  '-'-._'-./ -00- \.-'_.-'-'  `-'         ||     ├─→ SPRAY      #     ├─→ UFORST          ||
        _|  ||  '-.____||____.-'  || | _          ||     ├─→ SMURF      #     ├─→ DROPER          ||
     .' _ |  |╞══O |    __    | O══╡| | _ '.      ||     ├─→ TACHYON    #     ├─→ OVERLAP         ||
    / .' ''.|   || | /_00_\ | ||  |.'' '. \       ||     ├─→ MONLIST    #     ├─→ PINGER          ||
 _  | '###  |  ═╡ | ###### | |=  |' ###  |  _     ||     ├─→ FRAGGLE    #     ├─→ UFOUDP          ||
(0)─┤ |(0)| '.  0\||__**_ ||/0  .' |(0)| ├─(0)    ||     ├─→ SNIPER     #                         ||
 *  \ '._.'  '.  | \_##_/ |  .'  '._.' /  *       ||                                              ||
     '.__ _____0_'.|__'--'__|.'_0_____ __.'       #╞══════════════════════════════════════════════╡#
    .'_.─┤             YY            ├─._'.       ||                                              ||
                                                  ||  → [ UFONet: https://ufonet.03c8.net ] ←     ||
   + Class: PSYoPs / ViPR404+/(model:I^4*2) +     ||                                              ||
                                                  #╞══════════════════════════════════════════════╡#

═══════════════════════════════════════════════════════════════════════════

888     888 8888888888 .d88888b.  888b    888          888
888     888 888        d88P Y888b 8888b   888          888
888     888 888       888     888 88888b  888          888
888     888 8888888   888     888 888Y88b 888  .d88b.  888888
888     888 888       888     888 888 Y88b888 d8P  Y8b 888
888     888 888       888     888 888  Y88888 88888888 888
Y88b. .d88P 888       Y88b. .d88P 888   Y8888 Y8b.     Y88b.
 'Y88888P'  888        'Y88888P'  888    Y888  'Y8888   'Y8888

{(D)enial(OFF)ensive(S)ervice[ToolKit]}-{by_(io=psy+/03c8.net)}

═══════════════════════════════════════════════════════════════════════════

[AI] Downloading list of [Zombies] from [Private] server: DIP ...

══════════════════════

[AI] Trying [Blackhole] [Server]: DIP
```

OTHER TOOLS USED

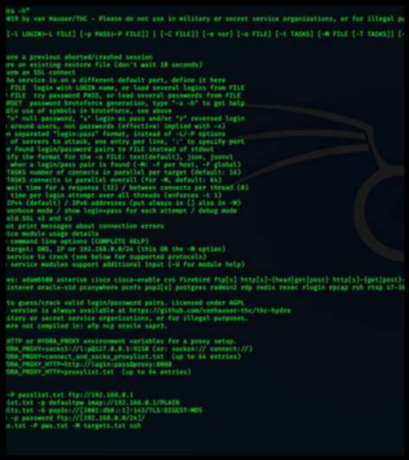
KALI LINUX

Tools used: -

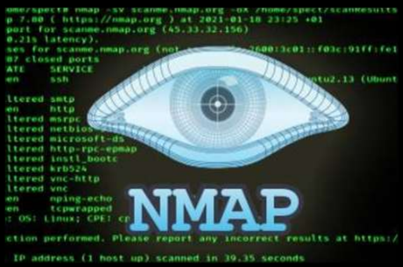
Theharvester, hydra, nmap, wireshark, autopsy, ngork, phoneinfoga, sqlmap, dnsenum, burpsuite, volatility, etc.



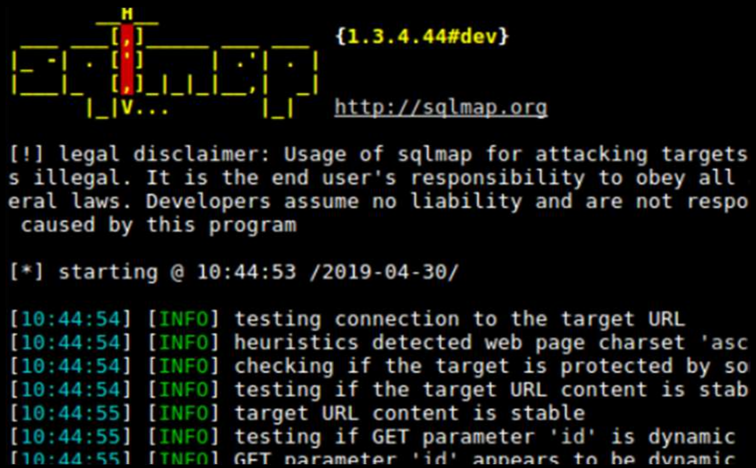
```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's do

*******************************************************************
*                                                                 *
*                                                                 *
* 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#
```



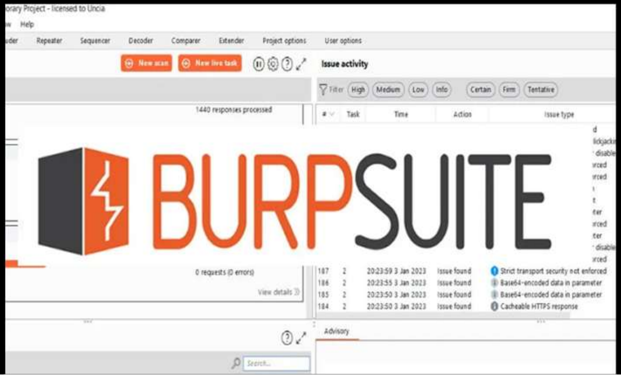
```
ra -h"
019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal p

[-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
07 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
```



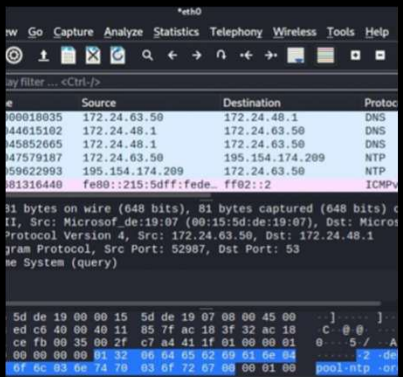
```
{1.3.4.44#dev}

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
```



1440 responses processed

0 requests (0 errors)

#	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
081316440     fe80::215:5dff:fede… ff02::2             ICMPv

81 bytes on wire (648 bits), 81 bytes captured (648 bits) o
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
```