AnonRoute – ANONYMOUS TRAFFIC ROUTING TOOL

by

AZADVIR SNGH

With the current era of digital surveillance and network monitoring, it has been increasingly challenging to protect online anonymity and maintain privacy. Classic options like Virtual Private Networks (VPNs) and proxies give consumers some form of protection but nevertheless depend on a centralized server that can be attacked, monitored, and intervened against by governments. To reduce these threats, Anon-Route has been created—a robust and streamlined tool which takes advantage of the Tor network in order to supply anonymous, encrypted internet traffic to Linux users.

Anon-Route is a command-line application which allows the user to install a transparent proxy via the Tor network, ensuring all outbound traffic, whether an application or a protocol, will pass via Tor. Using Tor's Onion Routing method, the tool ensures that the IP address of the user is concealed and all the traffic is anonymized, such that it is virtually impossible for third parties to track the online activities of the user. The tool works by setting up iptables, which is a utility for establishing firewall rules on Linux, to divert traffic through Tor automatically without having to be manually configured by the user.

The core aim of this project is to offer a user-friendly, lightweight, open-source solution for passing internet traffic via the Tor network. Anon-Route focuses on meeting increasing demands for privacy-oriented tools, which are easy to deploy, secure by nature, and that need little manual intervention from the user. Anon-Route seeks to banish the simplicity of typical VPN configurations and supply an easy command-line interface for users to make their anonymity uncomplicated.

This project offers a concrete, real-life application for cyber security professionals, privacy-oriented users, and researchers who require securing anonymity at the network level and operating using Linux-based systems. It enables the user to enjoy their privacy without relying on central services so they can be obscured from observation or tracking processes. With this project, users come to better know network security, privacy practice, and applying safe communication protocols.

IMPLEMENTATION

The deployment phase of the AnonRoute project is converting the design architecture into a functional solution by employing Bash scripting on Linux. This chapter documents a detailed description of how different parts of the system were implemented, integrated, and tested to produce secure and anonymous routing of all traffic via the Tor network.

4.1 IMPLEMENTATION ENVIORMENT

The creation and testing of AnonRoute took place in a reproducing and controlled setting for reliability and compatibility assurance.

- **Platform**
    - Operating System: Kali Linux 2023.4 (penetration testing Debian-based distro)
    - Kernel Version: Linux kernel 6.x
    - Environment: VMware Workstation / VirtualBox virtualized environment
    - Execution Shell: GNU Bash (version 5.x)

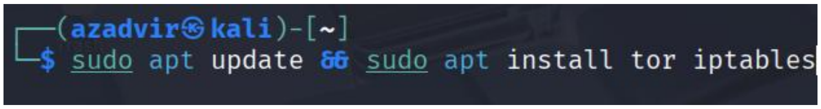
- **Tools and Utilities**
    - Tor – Executed as the principal anonymity network utility.
    - iptables – Utilized for redirection of traffic and firewall configuration.
    - netfilter-persistent – (Optional) To persist iptables rules on reboot.
    - whois / curl / wget – For IP verification and web requests.
    - ANSI escape codes – For colored, formatted CLI output.

4.2 IMPLEMENTATION STEPS

The process of implementing AnonRoute is divided into several functional modules, each handling a particular feature of the tool.

1. Project Setup

- Installed all required dependencies using:

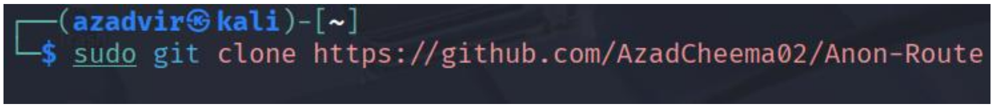


```
┌──(azadvir㉿kali)-[~]
└─$ sudo apt update && sudo apt install tor iptables
```

Figure 1. Setup commands

- Verified that the tor service is enabled and properly configured to listen on:
  - TransPort: 9040
  - DNSPort: 5353

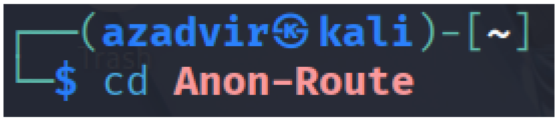
2. Downloading AnonRoute From Github



```
┌──(azadvir㉿kali)-[~]
└─$ sudo git clone https://github.com/AzadCheema02/Anon-Route
```

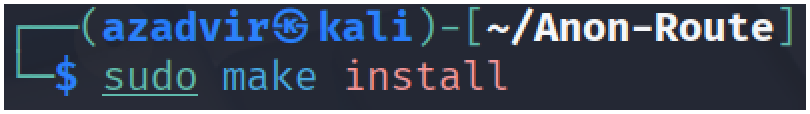
Figure 2. Downloading Repository from GitHub

3. Enter Anon-Route Directory and Install it



```
┌──(azadvir㉿kali)-[~]
└─$ cd Anon-Route
```

Figure 3. Navigating Anon-Route



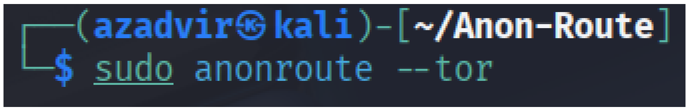
```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo make install
```

Figure 4. Installing Anon-Route

4. Commands

a. Start transparent proxy through Anon-Route

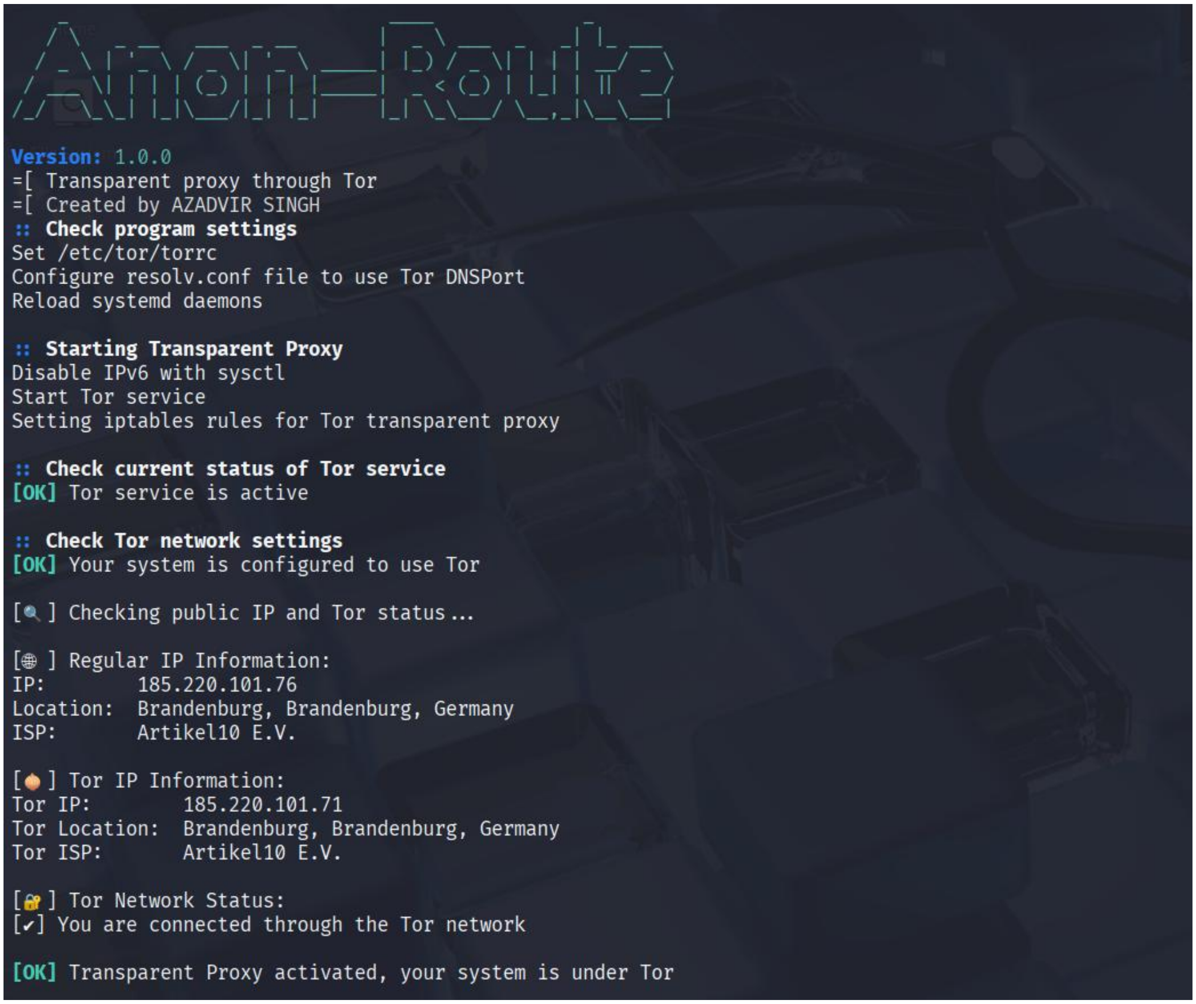
<sudo anonrote -t> or <sudo anonroute --tor>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --tor
```

Figure 5. Command 1 Starting TOR Proxy

- **OUTPUT:**

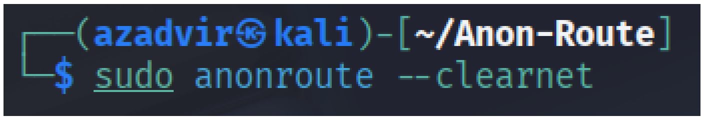


```
Version: 1.0.0
=[ Transparent proxy through Tor
=[ Created by AZADVIR SINGH
:: Check program settings
Set /etc/tor/torrc
Configure resolv.conf file to use Tor DNSPort
Reload systemd daemons

:: Starting Transparent Proxy
Disable IPv6 with sysctl
Start Tor service
Setting iptables rules for Tor transparent proxy

:: Check current status of Tor service
[OK] Tor service is active

:: Check Tor network settings
[OK] Your system is configured to use Tor

[🔍] Checking public IP and Tor status...

[🌐] Regular IP Information:
IP:         185.220.101.76
Location:   Brandenburg, Brandenburg, Germany
ISP:        Artikel10 E.V.

[🧅] Tor IP Information:
Tor IP:         185.220.101.71
Tor Location:   Brandenburg, Brandenburg, Germany
Tor ISP:        Artikel10 E.V.

[🔐] Tor Network Status:
[✓] You are connected through the Tor network

[OK] Transparent Proxy activated, your system is under Tor
```

Figure 6. Anon-Route Interface

b. Reset iptables and return to Clearnet navigation

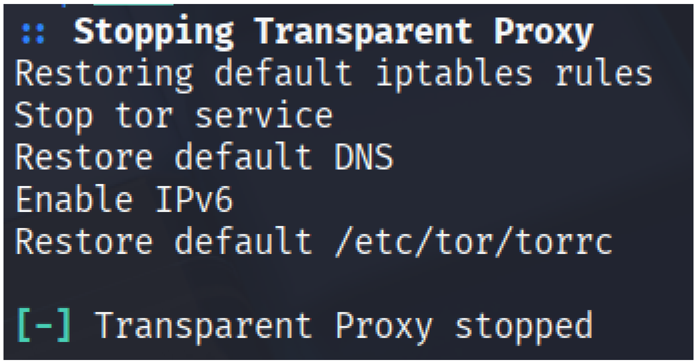
<sudo anonrote -c> or <sudo anonroute --clearnet>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --clearnet
```

Figure 7. Command 2 Clearnet Navigation

- **OUTPUT:**

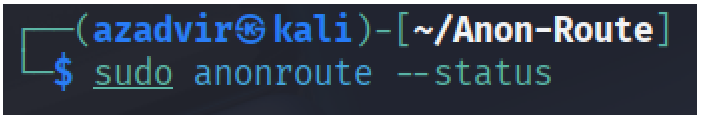


```
:: Stopping Transparent Proxy
Restoring default iptables rules
Stop tor service
Restore default DNS
Enable IPv6
Restore default /etc/tor/torrc

[-] Transparent Proxy stopped
```

Figure 8. Command 2 Output

c. **Check status of program and services**

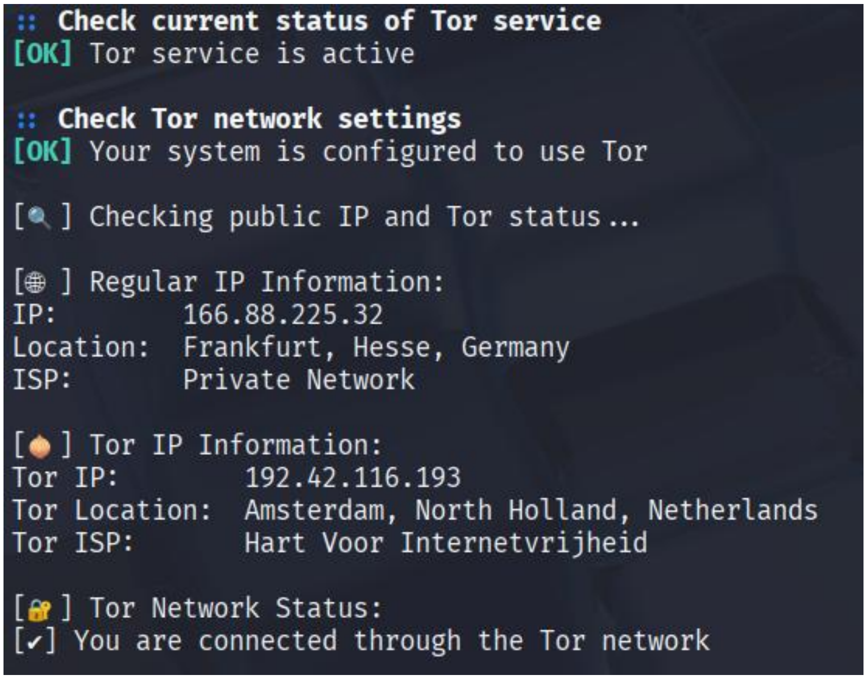
<sudo anonrote -s> or <sudo anonroute --status>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --status
```

Figure 9. Command 3 Checking Status

OUTPUT

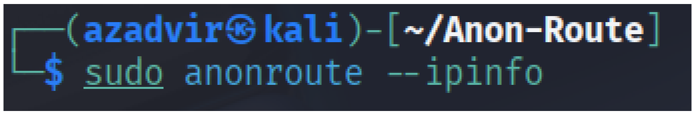


```
:: Check current status of Tor service
[OK] Tor service is active

:: Check Tor network settings
[OK] Your system is configured to use Tor

[🔍] Checking public IP and Tor status...

[🌐] Regular IP Information:
IP:         166.88.225.32
Location:   Frankfurt, Hesse, Germany
ISP:        Private Network

[🧅] Tor IP Information:
Tor IP:         192.42.116.193
Tor Location:   Amsterdam, North Holland, Netherlands
Tor ISP:        Hart Voor Internetvrijheid

[🔐] Tor Network Status:
[✓] You are connected through the Tor network
```

Figure 10 Command 3 Output

d. Show public IP address

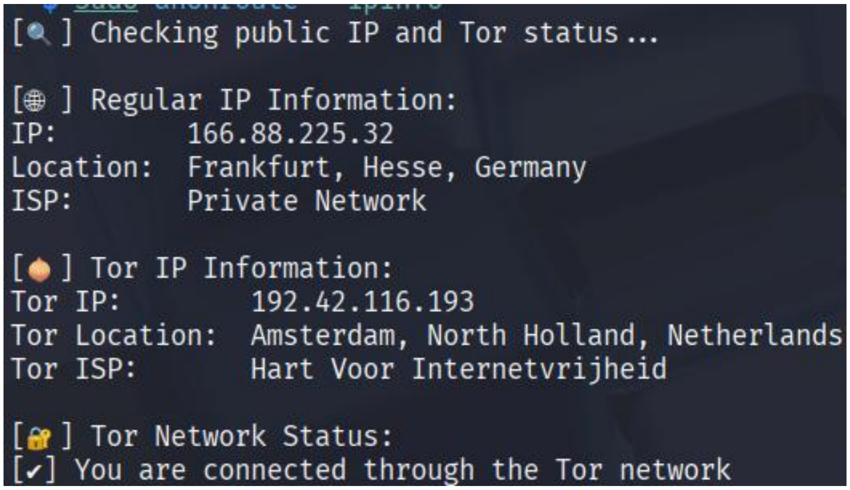
<sudo anonrote -i > or <sudo anonroute --ipinfo>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --ipinfo
```

Figure 11. Command 4 IP Information

OUTPUT

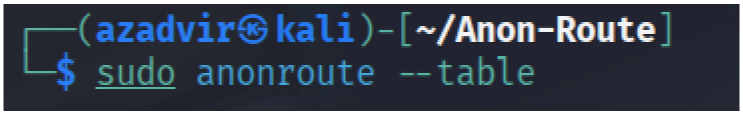


```
$ sudo anonroute --ipinfo
[🔍] Checking public IP and Tor status...

[🌐] Regular IP Information:
IP:         166.88.225.32
Location:   Frankfurt, Hesse, Germany
ISP:        Private Network

[🧅] Tor IP Information:
Tor IP:         192.42.116.193
Tor Location:   Amsterdam, North Holland, Netherlands
Tor ISP:        Hart Voor Internetvrijheid

[🔐] Tor Network Status:
[✓] You are connected through the Tor network
```

Figure 12. Command 4 Output

e. Display current IP Table Rules

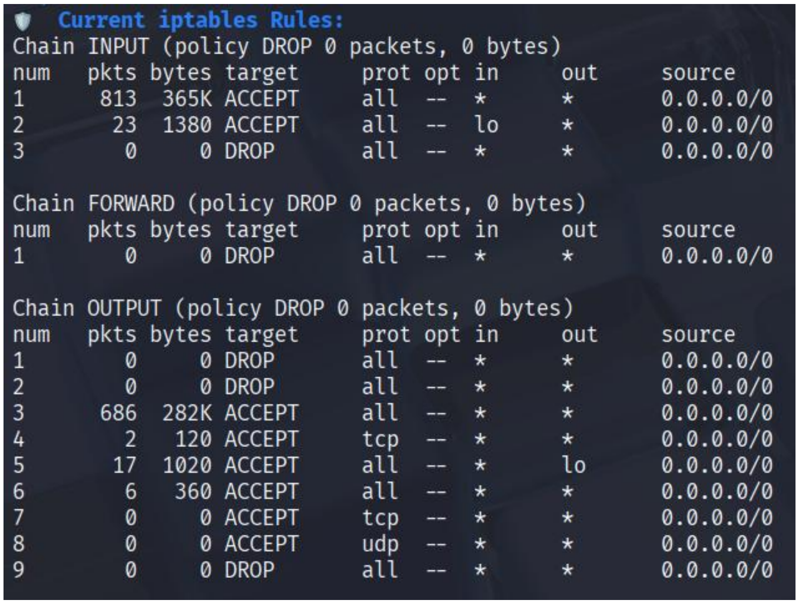
<sudo anonrote -tb> or <sudo anonroute --table>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --table
```

Figure 13. Command 5 Showing IP Table Rules

OUTPUT

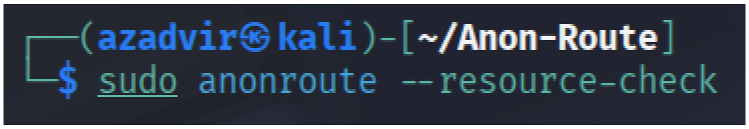


```
🛡 Current iptables Rules:
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source
1      813  365K ACCEPT     all  --  *      *       0.0.0.0/0
2       23  1380 ACCEPT     all  --  lo     *       0.0.0.0/0
3        0     0 DROP       all  --  *      *       0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source
1        0     0 DROP       all  --  *      *       0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source
1        0     0 DROP       all  --  *      *       0.0.0.0/0
2        0     0 DROP       all  --  *      *       0.0.0.0/0
3      686  282K ACCEPT     all  --  *      *       0.0.0.0/0
4        2   120 ACCEPT     tcp  --  *      *       0.0.0.0/0
5       17  1020 ACCEPT     all  --  *      lo      0.0.0.0/0
6        6   360 ACCEPT     all  --  *      *       0.0.0.0/0
7        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0
8        0     0 ACCEPT     udp  --  *      *       0.0.0.0/0
9        0     0 DROP       all  --  *      *       0.0.0.0/0
```

Figure 14. IP Table Rules

f. Display system's CPU, RAM, and disk usage performance

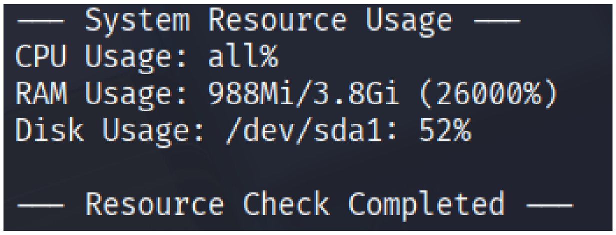
<sudo anonrote -rc> or <sudo anonroute –resource-check>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --resource-check
```

Figure 15. Command 6 Resource Check

OUTPUT

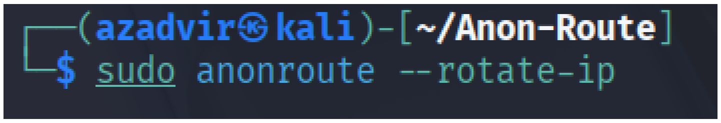


```
--- System Resource Usage ---
CPU Usage: all%
RAM Usage: 988Mi/3.8Gi (26000%)
Disk Usage: /dev/sda1: 52%

--- Resource Check Completed ---
```

Figure 16. System Performance

g. Rotate the Tor IP automatically after 10 seconds

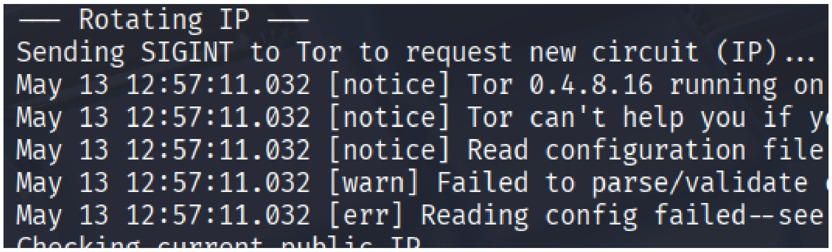
<sudo anonrote -rip> or <sudo anonroute –rotate-ip>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --rotate-ip
```

Figure 17. Command 7 Rotating IP

OUTPUT

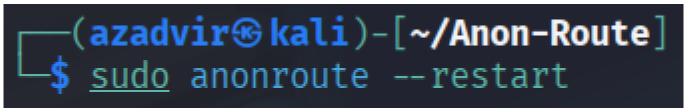


```
--- Rotating IP ---
Sending SIGINT to Tor to request new circuit (IP)...
May 13 12:57:11.032 [notice] Tor 0.4.8.16 running on
May 13 12:57:11.032 [notice] Tor can't help you if y
May 13 12:57:11.032 [notice] Read configuration file
May 13 12:57:11.032 [warn] Failed to parse/validate
May 13 12:57:11.032 [err] Reading config failed--see
Checking current public IP
```

Figure 18. Command 7 Output

h. Restart tor service and change IP address

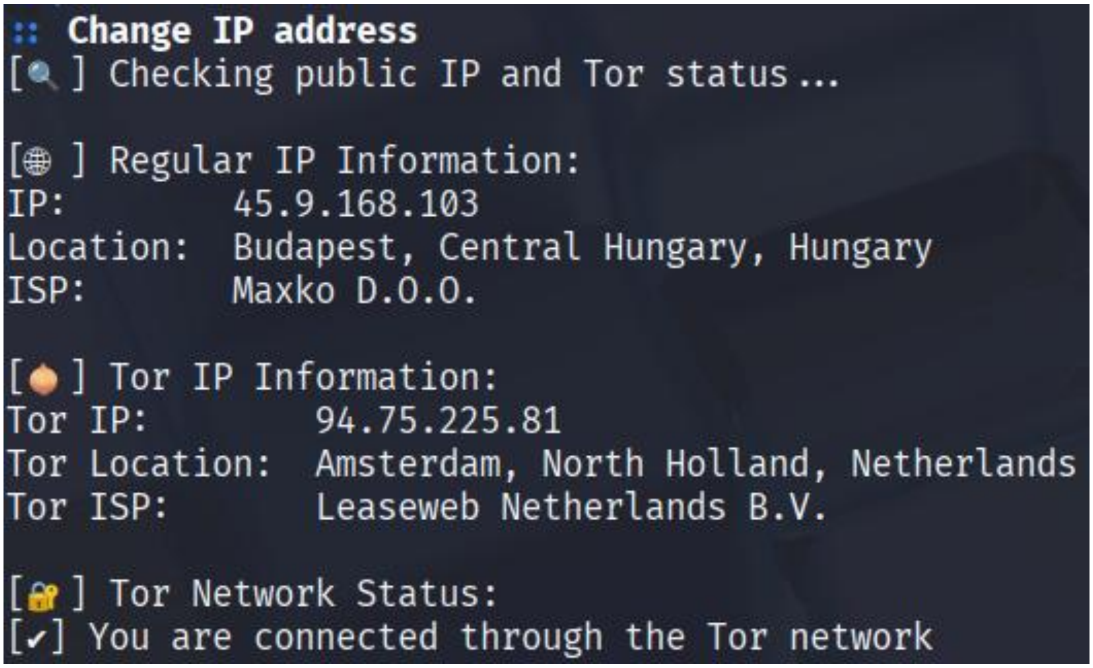
<sudo anonrote -r> or <sudo anonroute --restart>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --restart
```

Figure 19. Command 9 Restarting TOR services

OUTPUT

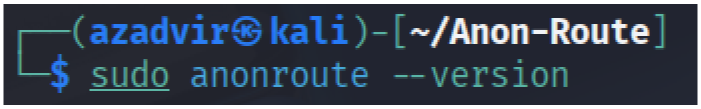


```
:: Change IP address
[🔍] Checking public IP and Tor status...

[🌐] Regular IP Information:
IP:          45.9.168.103
Location:    Budapest, Central Hungary, Hungary
ISP:         Maxko D.O.O.

[🧅] Tor IP Information:
Tor IP:          94.75.225.81
Tor Location:    Amsterdam, North Holland, Netherlands
Tor ISP:         Leaseweb Netherlands B.V.

[🔐] Tor Network Status:
[✓] You are connected through the Tor network
```

Figure 20. Command 9 Output

i. **Display program version and exit**

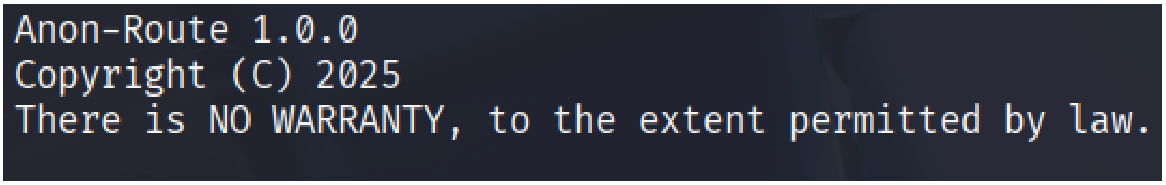
<sudo anonrote -v> or <sudo anonroute --version>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --version
```

Figure 21. Command 10 Version

OUTPUT

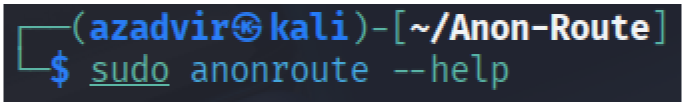


```
Anon-Route 1.0.0
Copyright (C) 2025
There is NO WARRANTY, to the extent permitted by law.
```

Figure 22. Current version of Anon-Route

j. **Help Message for learners**

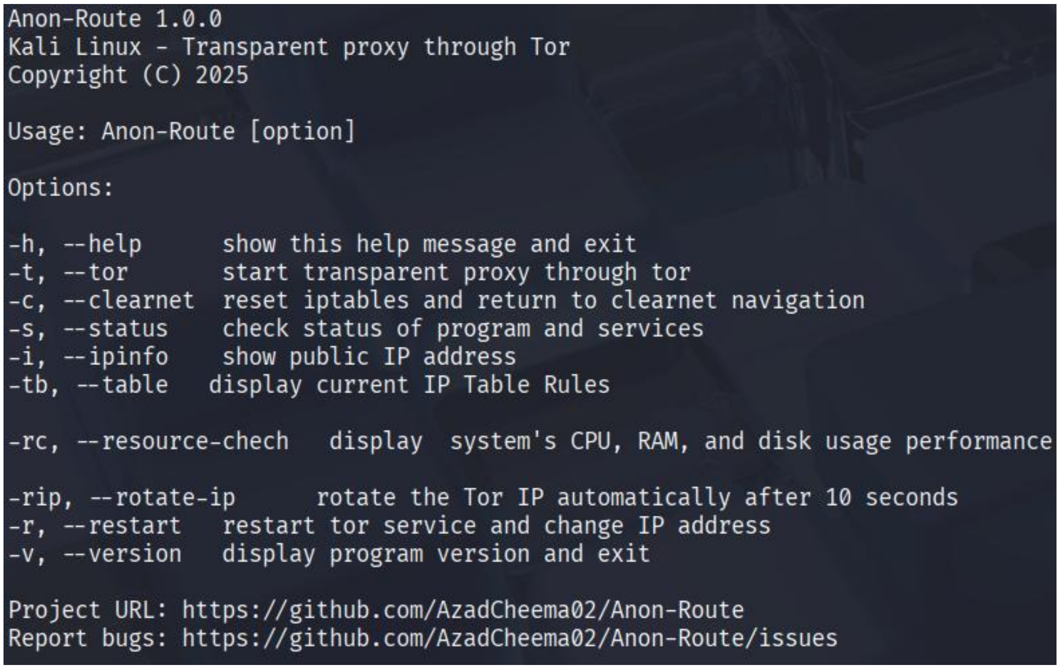
<sudo anonrote -h> or <sudo anonroute --help>



```
┌──(azadvir㉿kali)-[~/Anon-Route]
└─$ sudo anonroute --help
```

Figure 23 Command 9 Show Help Menu

OUTPUT

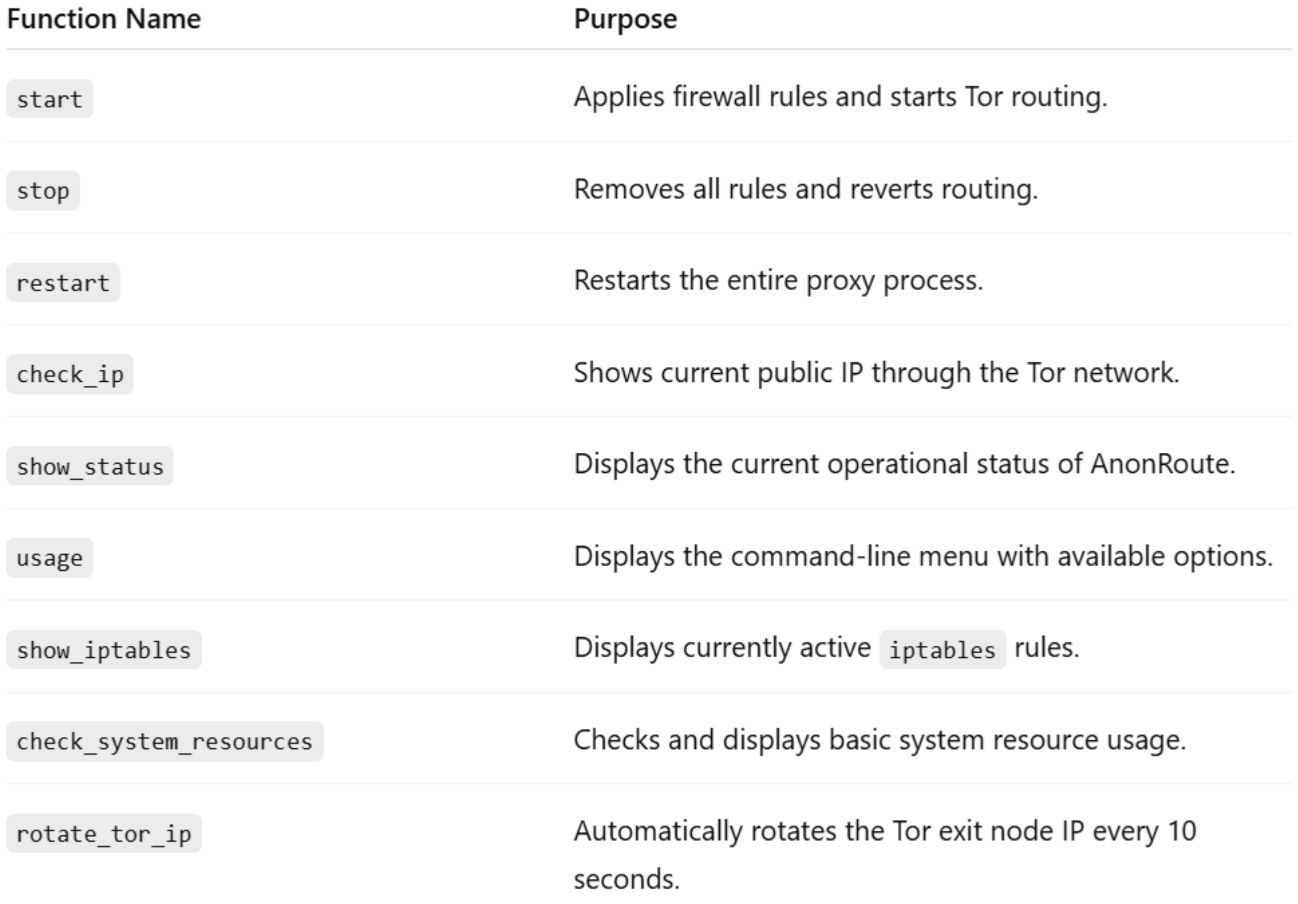


```
Anon-Route 1.0.0
Kali Linux - Transparent proxy through Tor
Copyright (C) 2025

Usage: Anon-Route [option]

Options:

-h, --help      show this help message and exit
-t, --tor       start transparent proxy through tor
-c, --clearnet  reset iptables and return to clearnet navigation
-s, --status    check status of program and services
-i, --ipinfo    show public IP address
-tb, --table   display current IP Table Rules

-rc, --resource-chech   display  system's CPU, RAM, and disk usage performance

-rip, --rotate-ip      rotate the Tor IP automatically after 10 seconds
-r, --restart   restart tor service and change IP address
-v, --version   display program version and exit

Project URL: https://github.com/AzadCheema02/Anon-Route
Report bugs: https://github.com/AzadCheema02/Anon-Route/issues
```

Figure 24. Help Menu

4.3 SCRIPT MODULARIZATION

Table 4-0-1 Script Modularization



Function Name	Purpose
`start`	Applies firewall rules and starts Tor routing.
`stop`	Removes all rules and reverts routing.
`restart`	Restarts the entire proxy process.
`check_ip`	Shows current public IP through the Tor network.
`show_status`	Displays the current operational status of AnonRoute.
`usage`	Displays the command-line menu with available options.
`show_iptables`	Displays currently active `iptables` rules.
`check_system_resources`	Checks and displays basic system resource usage.
`rotate_tor_ip`	Automatically rotates the Tor exit node IP every 10 seconds.

4.4ERROR HANDELING AND VALIDATIONS

- **Dependency Checks:** The user is notified and the script terminates if tor or iptables is not found.
- **Root Privilege Check:** The script inspects for root privileges and refuses to run if it is not run as root or with the use of sudo.
- **Tor Service Failure:** The script notifies the user if the Tor service doesn't start, instructing the user to check the service logs manually.
- **Invalid Input:** If the user has entered an invalid menu option, a warning message is shown and the menu is refreshed.

4.5 SECURITY CONSIDERATION

- All non-Tor outgoing traffic is blocked so that there will be zero leaks.
- DNS leaks are avoided by forwarding DNS requests through Tor's DNSPort.
- Whitelisting just Tor's UID prevents an attempt to establish a routing loop for Tor's own traffic.
- The script won't store user data or log anything, making it private

4.6 IMPROVEMENTS FROM PREVIOUS TOOLS

- Compared to tools like Kalitorify or toriptables2, **AnonRoute**:
  - Uses reduced logic and fewer dependencies.
  - Delivers immediate status feedback.
  - Maintenance of modular functions is significantly easier.
  - Includes additional functionality such as restart and IP validation.

CONCLUSION

SUMMARY OF THE PROJECT

The AnonRoute project was created with the main objective of facilitating anonymous web surfing by directing all internet traffic through the Tor network via a transparent proxy mechanism. The tool was written as a Bash shell script specifically for Kali Linux, which automated the setup of iptables, the Tor service, and DNS leak protection to provide privacy and anonymity.

During this project, the tool exhibited features such as:

- Autmatically launching and closing the Tor-based proxy.
- Redirecting all TCP traffic to use Tor.
- Avoiding DNS leaks by making DNS resolution occur through Tor.
- Enabling checking the users current public IP to confirm anonymity.
- Having a lightweight and easy-to-use command-line interface.

The project was successfully completed and shown to be useful in enhancing privacy on the Internet by hiding the actual IP address and blocking leakage of traffic out of the Tor network.

KEY OUTCOMES

- **Secure and Anonymous Routing:** AnonRoute offered a trustworthy means of anonymizing internet traffic via Tor.
- **Automated Setup:** All system-level settings required for the tool were automated, so it was available even to users with minimal technical

expertise.

- **DNS Leak Protection:** By sending DNS requests via Tor, AnonRoute prevented DNS leaks that would reveal user anonymity.
- **User Control:** The software gave users the convenience to initiate, shut down, reboot, and observe their anonymous routing configuration seamlessly.

FUTURE WORK

- **Graphical User Interface (GUI):** Including a GUI frontend for simpler interaction.
- **Multi-platform Support:** Expanding support to other Linux distributions and even Windows with WSL.
- **Advanced Traffic Routing:** Allowing user-specified applications to route selectively over Tor while leaving others on the normal network
- **Integration with VPN:** Merging Tor with VPN layers for increased anonymity.

FINAL WORDS

AnonRoute is a solid foundation for privacy-oriented users and researchers who seek to investigate secure traffic routing through open-source networks such as Tor. As privacy concerns expand around the world, technologies such as AnonRoute help create a protective barrier against surveillance, tracking, and censorship. This project not only fulfills technical requirements but also helps promote the ethical significance of digital freedom.