# How to Use Stubby to Enhance DNS Privacy in Linux

Stubby is a DNS privacy tool that encrypts DNS queries between your computer and the DNS resolver. It helps protect your online privacy by preventing eavesdropping and manipulation of your DNS traffic. Stubby is particularly useful in Linux environments where privacy and security are of utmost importance.

By default, Linux systems use a DNS resolver provided by the Internet Service Provider (ISP) or a public DNS resolver like Google DNS. However, these DNS resolvers may not prioritize privacy and can potentially log your DNS queries, exposing your browsing habits to third parties. Stubby acts as a local DNS resolver that encrypts your DNS queries and forwards them to a trusted DNS resolver, ensuring your privacy is maintained.

To use Stubby in Linux, follow these steps:

1. Install Stubby:
    - Open a terminal.
    - Update the package list: sudo apt update
    - Install Stubby: sudo apt install stubby
2. Configure Stubby:
    - Open the Stubby configuration file using a text editor: sudo nano /etc/stubby/stubby.yml
    - Customize the configuration based on your preferences. You can specify the DNS resolvers you trust, enable DNS-over-TLS or DNS-over-HTTPS, and configure other options.
    - Save the changes and exit the text editor.
3. Start and enable Stubby:
    - Start the Stubby service: sudo systemctl start stubby
    - Enable Stubby to start on boot: sudo systemctl enable stubby
4. Verify Stubby is working:
    - Open a web browser and visit a website.
    - Open a terminal and run the following command to check the DNS resolver used by your system: systemd-resolve --status | grep 'DNS Servers'
    - If the output includes the IP addresses of the DNS resolvers you specified in the

Stubby configuration file, Stubby is working correctly.