

USER PRIVACY IN LINUX





Contents

Introduction	3
Secure OS Installation	3
Steps:.....	3
Removing the packages	14
Settings in ubuntu	15
Disable diagnostics reporting.....	15
Disable lock screen notifications.....	15
Disable tracking of recent files.....	16
Turning off the problem reporting	17
Turning off the screen blank	18
Disable automatic screen locking.....	19
Permanently delete option	20
Show hidden files.....	21
BleachBit	21
KeePassXC	22
Virus Scanner	23
Metadata removal.....	24
Firefox profilemaker.....	25
Flatpak.....	26
LibreWolf.....	26
VeraCrypt	27
Tor Browser	29
Proton VPN.....	31
NextDNS	34
Conclusion.....	40



Introduction

Linux telemetry, which involves gathering and sending data from a Linux-based system to an external server or service, raises concerns about **Linux telemetry and privacy**. The purpose of this process is often to monitor system performance, provide diagnostics, enable analytics, or improve system functionality. The collected data may encompass system performance indicators, usage patterns, hardware specifications, error logs, and other relevant information. In this article, we are going to discuss why telemetry can be seen as a potential threat to privacy, even when used for legitimate purposes. We will also explore methods to make the system more secure than before.

Secure OS Installation

Ideally, we should consider the **POP!_OS** by **System76** for installation, it is based on Ubuntu but redesigned for privacy and security. However, here we are considering the **Ubuntu 22.04.4** version. We are considering this version of Ubuntu because the versions which begin with an **odd number** or end with the **0.10** are **interim** releases with a short support cycle and we will be needing a version which has the Long Term Support (**LTS**). Hence only versions which begin with an **even number** and end with **0.04** should be considered. We will discuss the steps to make it secure from the installation itself.

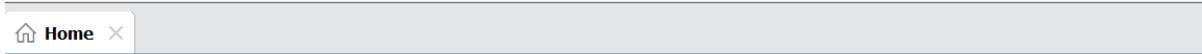
Steps:

- 1: Download the ubuntu-22.04.4-desktop-amd64.iso image from the following URL: <https://old-releases.ubuntu.com/releases/22.04/>



Name	Last modified	Size
Parent Directory		-
SHA256SUMS	2024-02-22 15:31	202
SHA256SUMS.gpg	2024-02-22 15:31	833
ubuntu-22.04.4-desktop-amd64.iso	2024-02-20 19:39	4.7G
ubuntu-22.04.4-desktop-amd64.iso.torrent	2024-02-22 15:31	374K
ubuntu-22.04.4-desktop-amd64.iso.zsync	2024-02-22 15:31	11M
ubuntu-22.04.4-desktop-amd64.list	2024-02-20 19:39	26K
ubuntu-22.04.4-desktop-amd64.manifest	2024-02-20 19:34	60K
ubuntu-22.04.4-live-server-amd64.iso	2024-02-16 23:52	2.0G
ubuntu-22.04.4-live-server-amd64.iso.torrent	2024-02-22 15:24	157K
ubuntu-22.04.4-live-server-amd64.iso.zsync	2024-02-22 15:24	3.9M
ubuntu-22.04.4-live-server-amd64.list	2024-02-16 23:52	7.8K
ubuntu-22.04.4-live-server-amd64.manifest	2024-02-16 19:09	19K

2: Create a new virtual machine in VMware workstation PRO.



3: Select the path of the installer disc.



New Virtual Machine Wizard X

Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

Installer disc:
 DVD RW Drive (E:)

Installer disc image file (iso):
D:\OS Images\Linux OS\ubuntu-22.04-desktop-amd64. v Browse...

i Ubuntu 64-bit 22.04 detected.
This operating system will use Easy Install. ([What's this?](#))

I will install the operating system later.
The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

4: Enter the Full name, Username, Password and Confirm.



New Virtual Machine Wizard

**Easy Install Information**

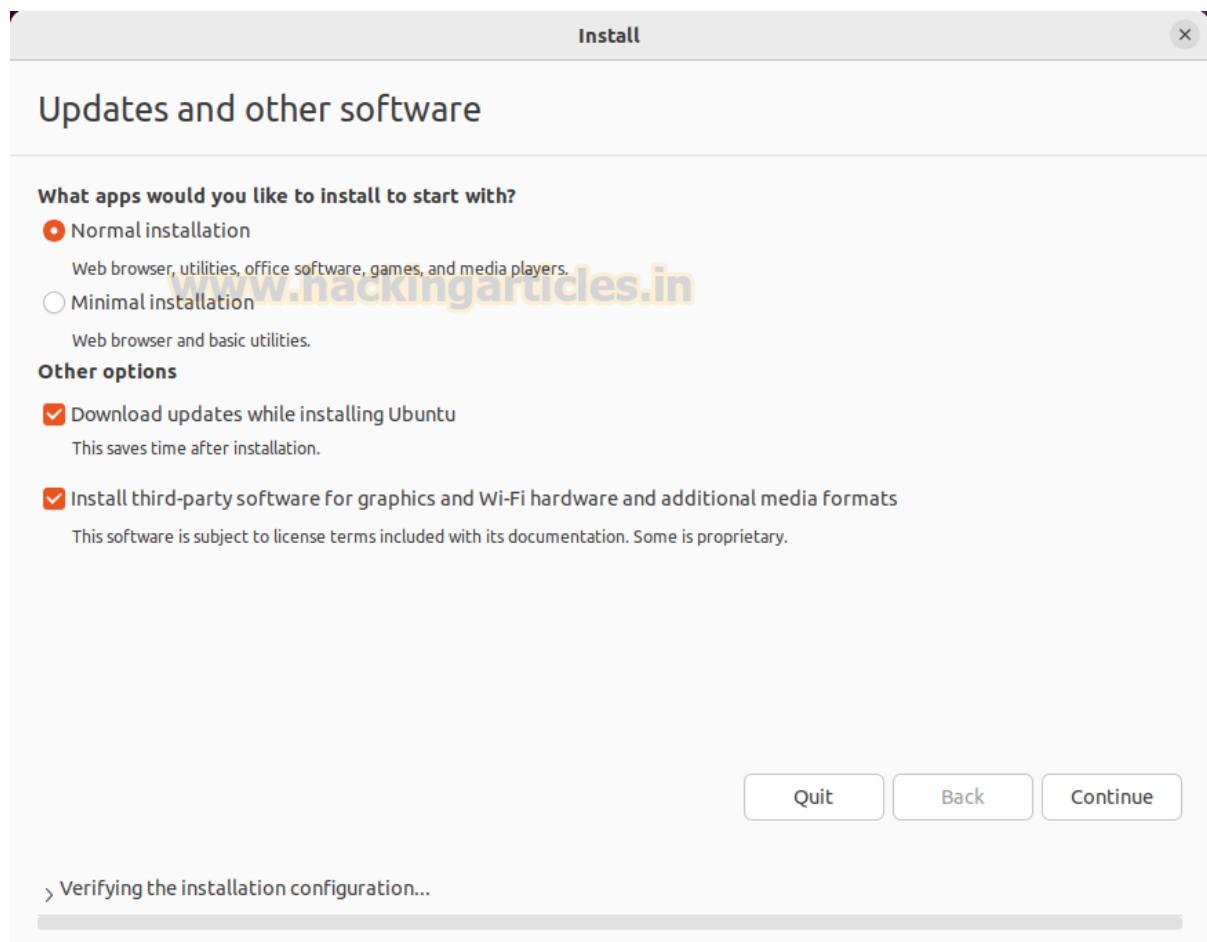
This is used to install Ubuntu 64-bit.

Personalize Linux

Full name: osint

User name: **osint**Password: **•••**Confirm: **•••**[Help](#)[< Back](#)[Next >](#)[Cancel](#)

5: Select the Normal installation and select both options in the Other options.



6: Select Erase disk and install Ubuntu, click on Advanced features.



Install X

Installation type

This computer currently has no detected operating systems. What would you like to do?

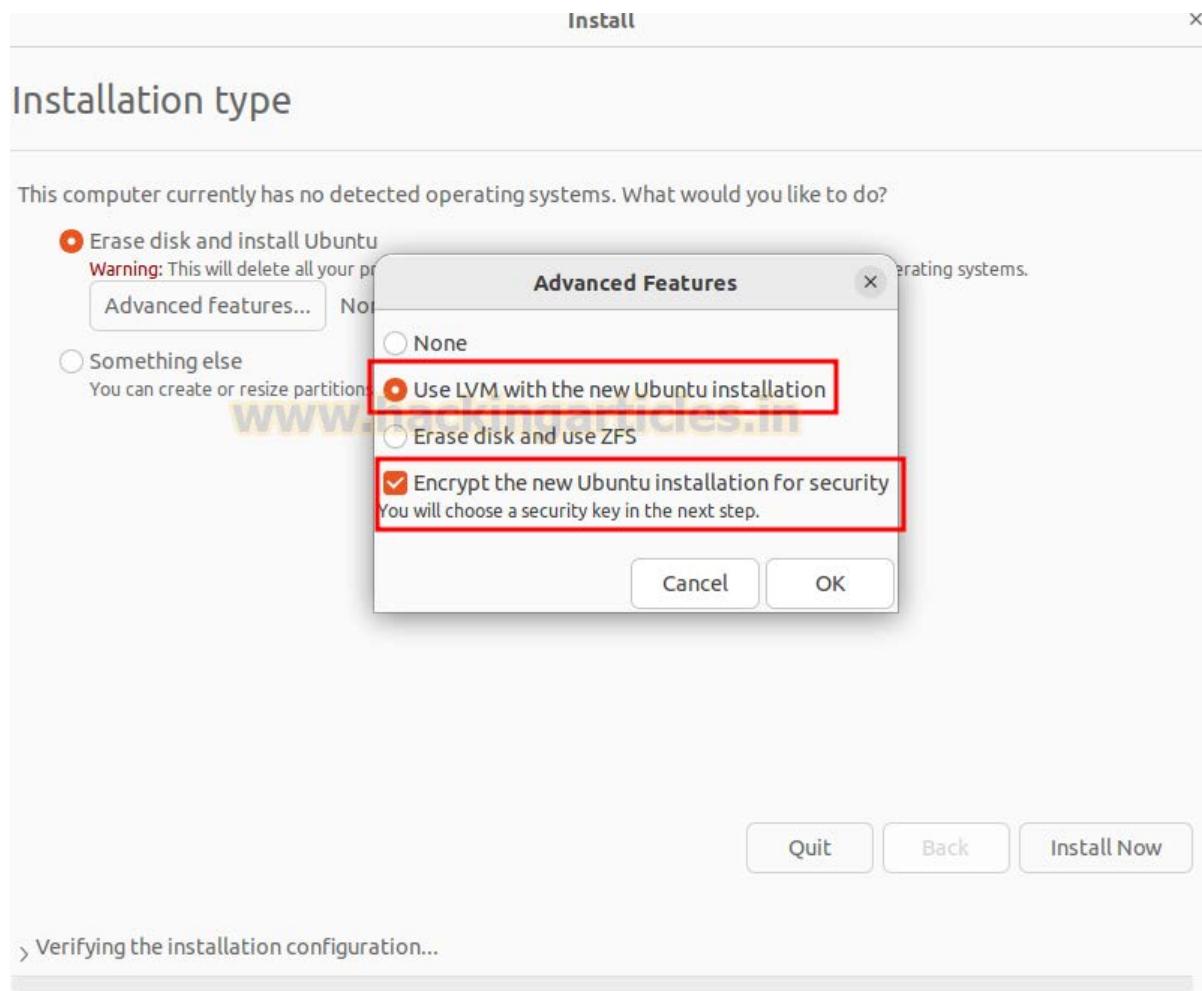
Erase disk and install Ubuntu
Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.
Advanced features... None selected

Something else
You can create or resize partitions yourself, or choose multiple partitions for Ubuntu.

[Quit](#) [Back](#) [Install Now](#)

› Verifying the installation configuration...

7: Inside Advanced features, use the following options: Use LVM with the new Ubuntu installation and Encrypt the new Ubuntu installation for Security.



8: Enter the Security key and click on Install now.



Install X

Choose a security key:

Disk encryption protects your files in case you lose your computer. It requires you to enter a security key each time the computer starts up.
Any files outside of Ubuntu will not be encrypted.

Choose a security key: Good password

Confirm the security key: ✓

Enable recovery key: A recovery key is generated and will be temporarily saved on the live system. You can select an alternate location. Save this file and keep it in a safe place elsewhere before rebooting.

Recovery key: C

Confirm recovery key:

Location: /home/ubuntu/recovery.key Download

Warning: If you lose this security key, all data will be lost. If you need to, write down your key and keep it in a safe place elsewhere.

For more security: Overwrite empty disk space
The installation may take much longer.

Quit Back Install Now

> Verifying the installation configuration...

9: Select Continue for the Write the changes to disks? Option.



Install

Choose a security key:

Disk encryption protects your files in case you lose your computer. It requires you to enter a security key each time the computer starts up.

Any files outside of Ubuntu will not be encrypted.

Choose a security key: Good password

Write the changes to disks?

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

WARNING: This will destroy all data on any partitions you have removed as well as on the partitions that are going to be formatted.

The following partitions are going to be formatted:
LVM VG vgubuntu, LV root as ext4
LVM VG vgubuntu, LV swap_1 as swap
partition #2 of SCSI33 (0,0,0) (sda) as ESP

Wipe place elsewhere.

For more security: Overwrite empty disk space
The installation may take much longer.

Go Back Continue

Back Install Now

> Verifying the installation configuration...

10: Enter the details in the Who are you? Installation option.



Install

Who are you?

Your name: osint ✓

Your computer's name: ignite ✓
The name it uses when it talks to other computers.

Pick a username: osint ✓

Choose a password: Short password

Confirm your password: ✓

Log in automatically
 Require my password to log in

Use Active Directory

You'll enter domain and other details in the next step.

[Back](#) [Continue](#)

> Copying files...

Once the installation is complete, you will see an ubuntu login screen like the one shown below.



Removing the packages

After login into the ubuntu machine, we can remove all those packages, which somehow transfer the user/system information to an outside source either for improvement, feedback, or diagnostic purpose.

Starting with the **whoopsie** package, it is a crash reporting daemon designed to capture application crashes and send anonymized reports to the Ubuntu servers.

The command to remove its entire content is:

```
sudo apt purge apport-symptoms popularity-contest ubuntu-report whoopsie
```



```
osint@ignite:~$ sudo apt purge apport apport-symptoms popularity-contest ubuntu-report whoopsie
[sudo] password for osint:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'popularity-contest' is not installed, so not removed
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gdb gstreamer1.0-vaapi i965-va-driver intel-media-va-driver libaacs0 lib
  libcodec2-1.0 libdavids5 libdebginfo-common libdebginfofod libflashrom1 libflite1 libftdi1-2 libgme0
  librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsource-highlight-common libsource-hi
  libvidstab1.1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers mesa-
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  apport* apport-gtk* apport-symptoms* ubuntu-report* whoopsie*
```

We will also remove the **motd-news** package, it is responsible for delivering dynamic news messages as part of the **Message of the Day** (MOTD) system.

The command to remove its entire content is:

```
sudo rm /etc/update-motd.d/50-motd-news
```

```
osint@ignite:~$ sudo rm /etc/update-motd.d/50-motd-news
osint@ignite:~$
```

Settings in ubuntu

After removing the packages, we can now proceed with the essential settings in ubuntu, which can help us to be more secure. Here we are going to show it using the terminal and how the same can be done on the GUI.

Disable diagnostics reporting

Apport is a crash reporting tool found in Ubuntu and other Linux-based operating systems. Its primary function is to identify when programs crash, gather detailed information about the error, and create reports that assist in diagnosing and troubleshooting the problem.

Setting the app crash report to false does not give the apport crash pop-up notifications.

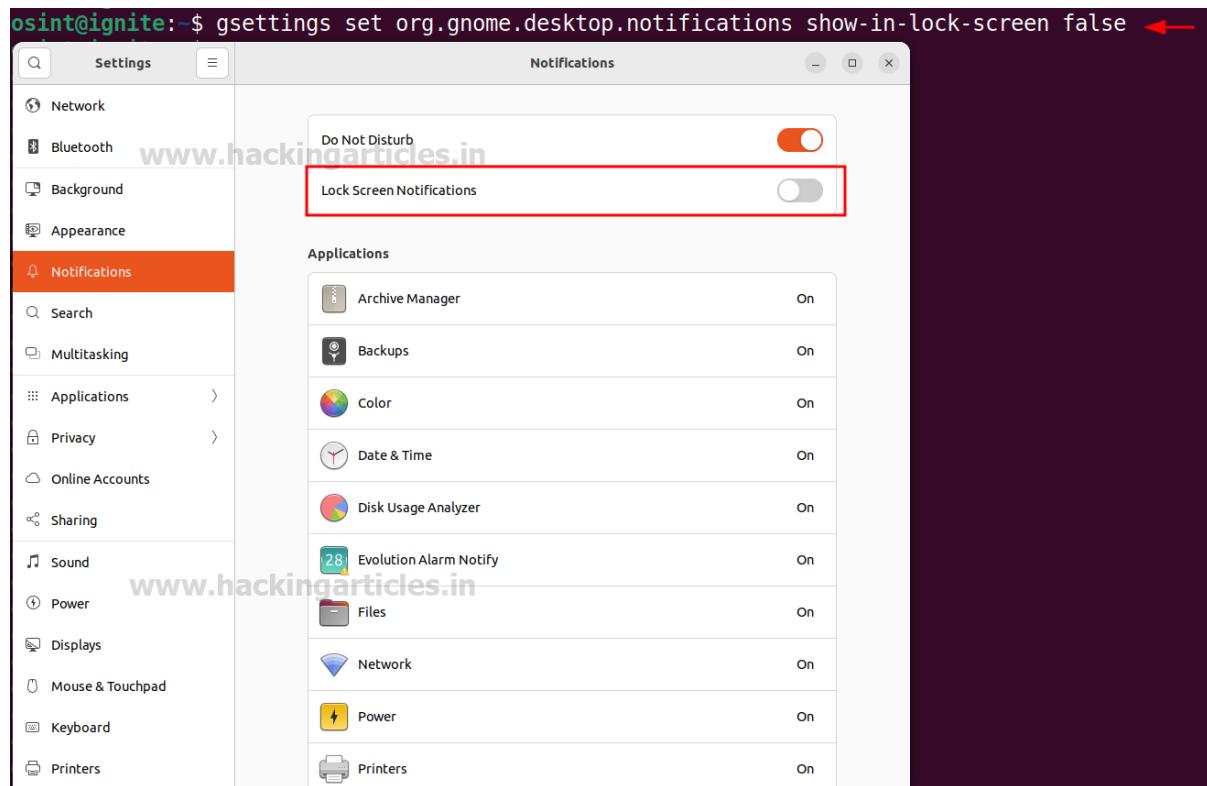
```
gsettings set com.ubuntu.update-notifier show-apport-crashes false
```

```
osint@ignite:~$ gsettings set com.ubuntu.update-notifier show-apport-crashes false
osint@ignite:~$
```

Disable lock screen notifications

Lock screen notifications can disclose various things which might be private to the user. So, we need to disable the lock screen notifications.

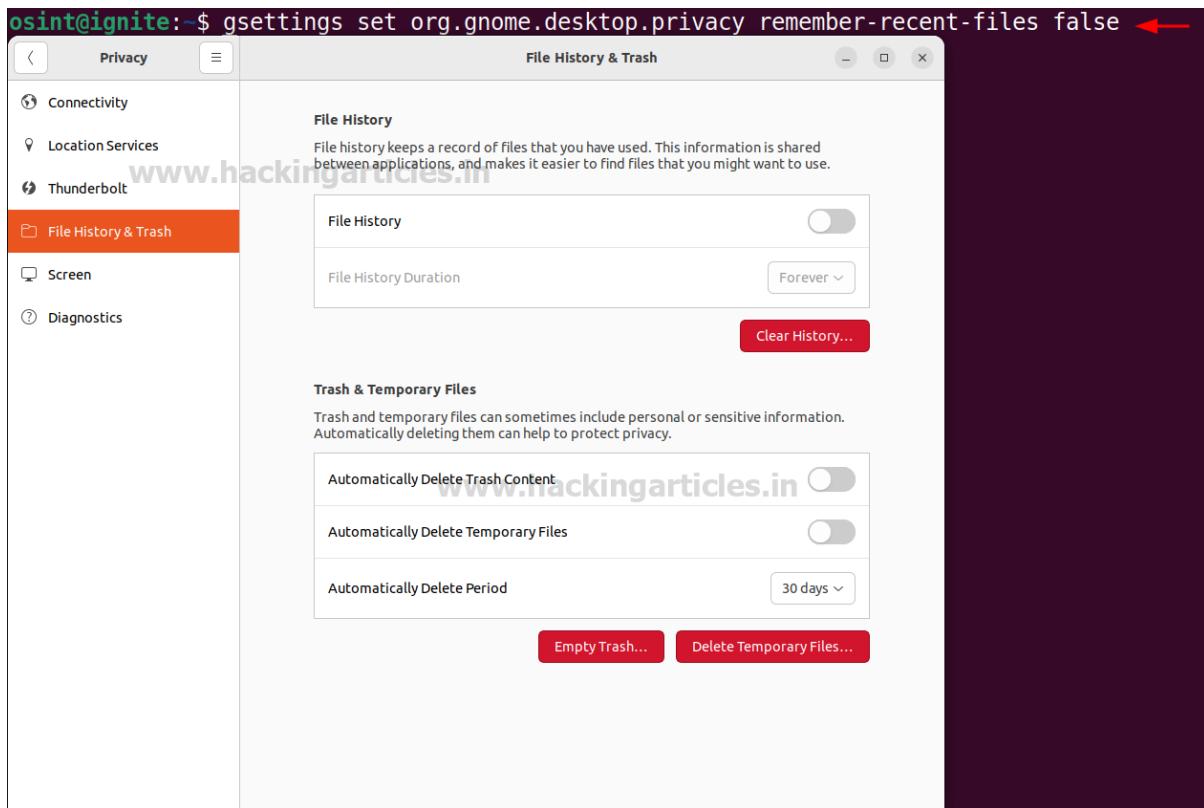
```
gsettings set org.gnome.desktop.notifications show-in-lock-screen false
```



Disable tracking of recent files

To disable the tracking of recently opened files in the ubuntu machine, we can set the **remember-recent-files** to **false**.

```
gsettings set org.gnome.desktop.privacy remember-recent-files false
```



Turning off the problem reporting

Open the Privacy setting in the GUI and inside Diagnostics set the **Send error reports to Canonical** to **Never**. By doing this no error reports will be shared to the Canonical and a privacy can be maintained.

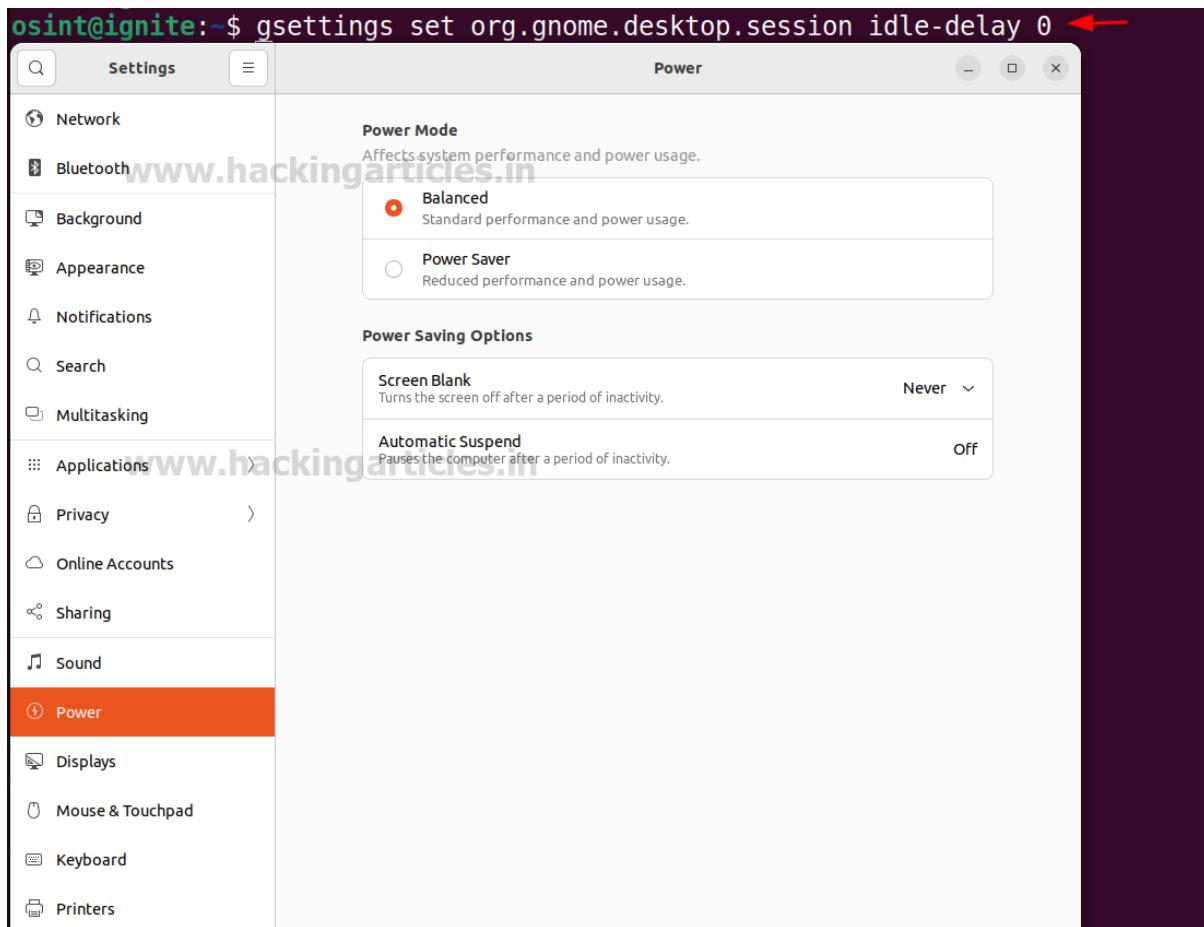


The screenshot shows the 'Privacy' settings window in Ubuntu. The left sidebar lists several categories: Connectivity, Location Services, Thunderbolt, File History & Trash, Screen, and Diagnostics. The 'Diagnostics' category is selected and highlighted with an orange background. The main content area is titled 'Problem Reporting' and contains the text: 'Sending reports of technical problems helps us improve Ubuntu. Reports are sent anonymously and are scrubbed of personal data.' Below this text is a dropdown menu labeled 'Send error reports to Canonical' with the option 'Never' selected. A red box highlights the 'Never' option.

Turning off the screen blank

To disable the automatic **screen blanking or locking due to inactivity**, first open the Power options. Then, set the **Screen Blank** option to **Never** and **Automatic Suspend** to **Off**. This way, the display stays on indefinitely because the inactivity action **never triggers**.

```
gsettings set org.gnome.desktop.session idle-delay 0
```



Disable automatic screen locking

To disable the automatic lock when the system remains idle, click the **Privacy** option, then click **Screen** and disable all options.

```
gsettings set org.gnome.desktop.screensaver lock-enabled false  
gsettings set org.gnome.desktop.screensaver ubuntu-lock-on-suspend false
```



The terminal window shows the following commands:

```
osint@ignite:~$ gsettings set org.gnome.desktop.screensaver lock-enabled false ←
osint@ignite:~$ gsettings set org.gnome.desktop.screensaver ubuntu-lock-on-suspend false ←
```

The GNOME Settings application window shows the 'Screen' tab selected. The 'Screen Lock' section contains the following settings:

- Blank Screen Delay: Set to Never.
- Automatic Screen Lock: Enabled (switch is on).
- Automatic Screen Lock Delay: Set to Screen Turns Off.
- Lock Screen on Suspend: Enabled (switch is on).
- Show Notifications on Lock Screen: Enabled (switch is on).

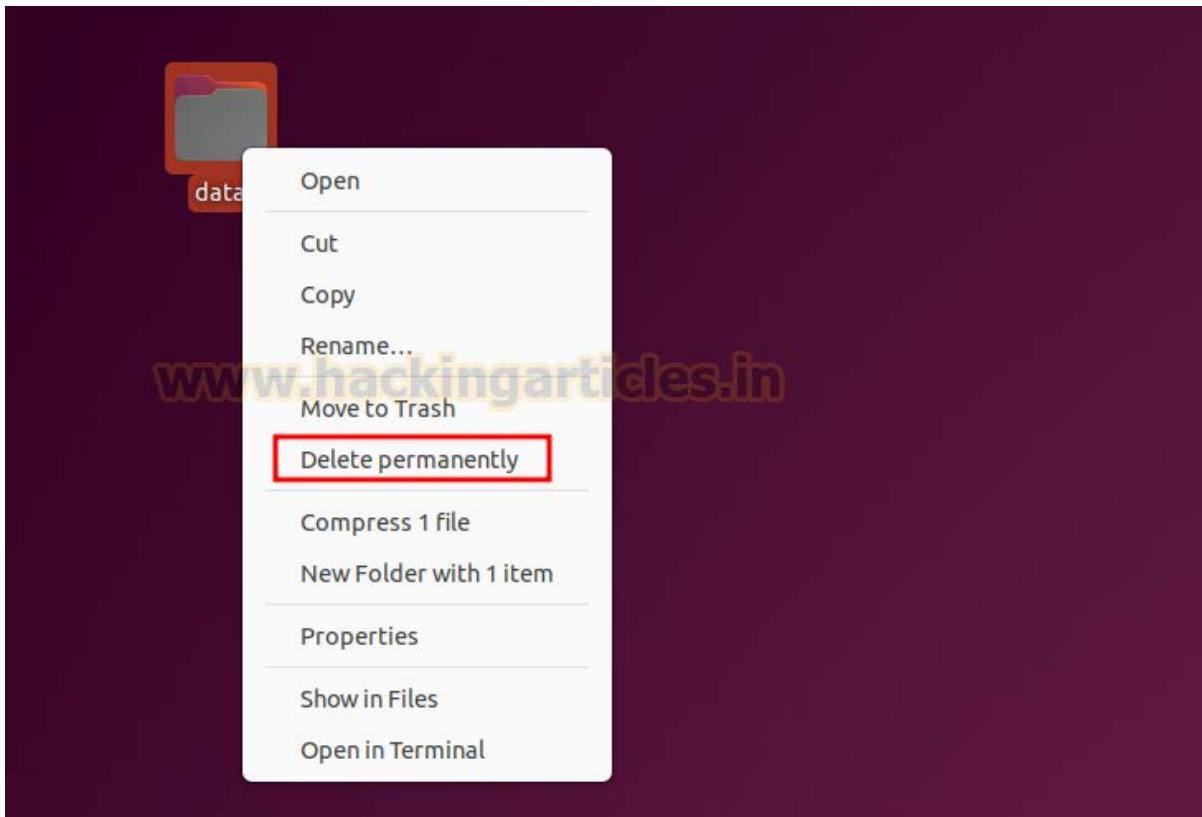
Permanently delete option

If we want to permanently delete an object without moving it to the trash, we can run the following command to get a permanently delete option for every file.

```
gsettings set org.gnome.nautilus.preferences show-delete-permanently true
```

```
osint@ignite:~$ gsettings set org.gnome.nautilus.preferences show-delete-permanently true ←
osint@ignite:~$
```

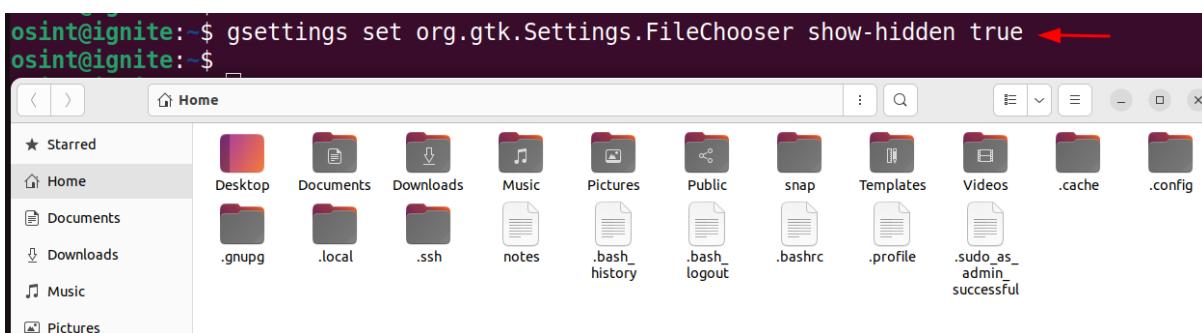
After running the above command, we can now see that we have **Delete permanently** option available for all the files.



Show hidden files

To permanently enable the view hidden files option, we can run the following command:

```
gsettings set org.gnome.nautilus.preferences show-hidden-files true
```



BleachBit

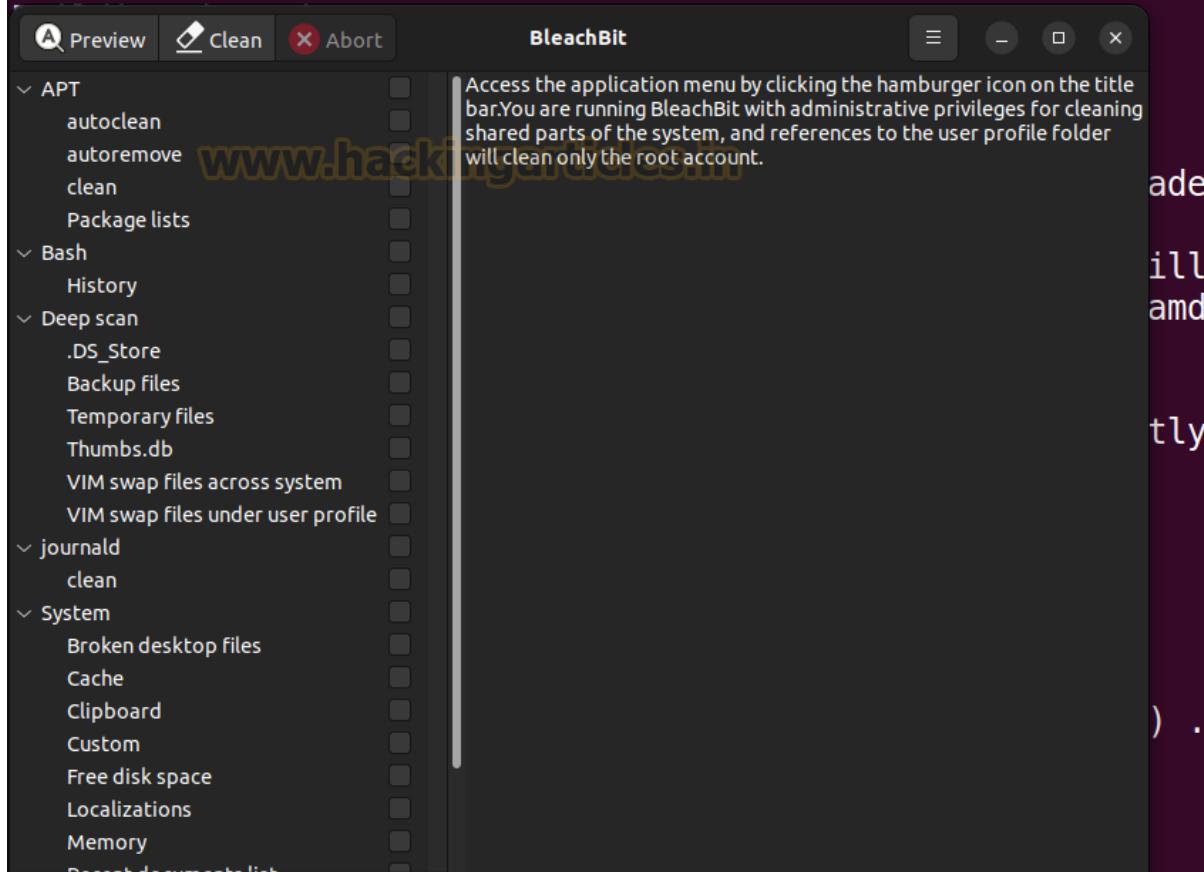
BleachBit is an **open-source application** that functions as a **system cleaner** and **privacy tool**. It **optimizes** disk space and **safeguards user privacy** by eliminating unwanted files and data from your computer.

Installation of BleachBit can be performed using the following command:

```
sudo apt install bleachbit
```



```
osint@ignite:~$ sudo apt install bleachbit ←  
[sudo] password for osint:  
Reading package lists... Done
```

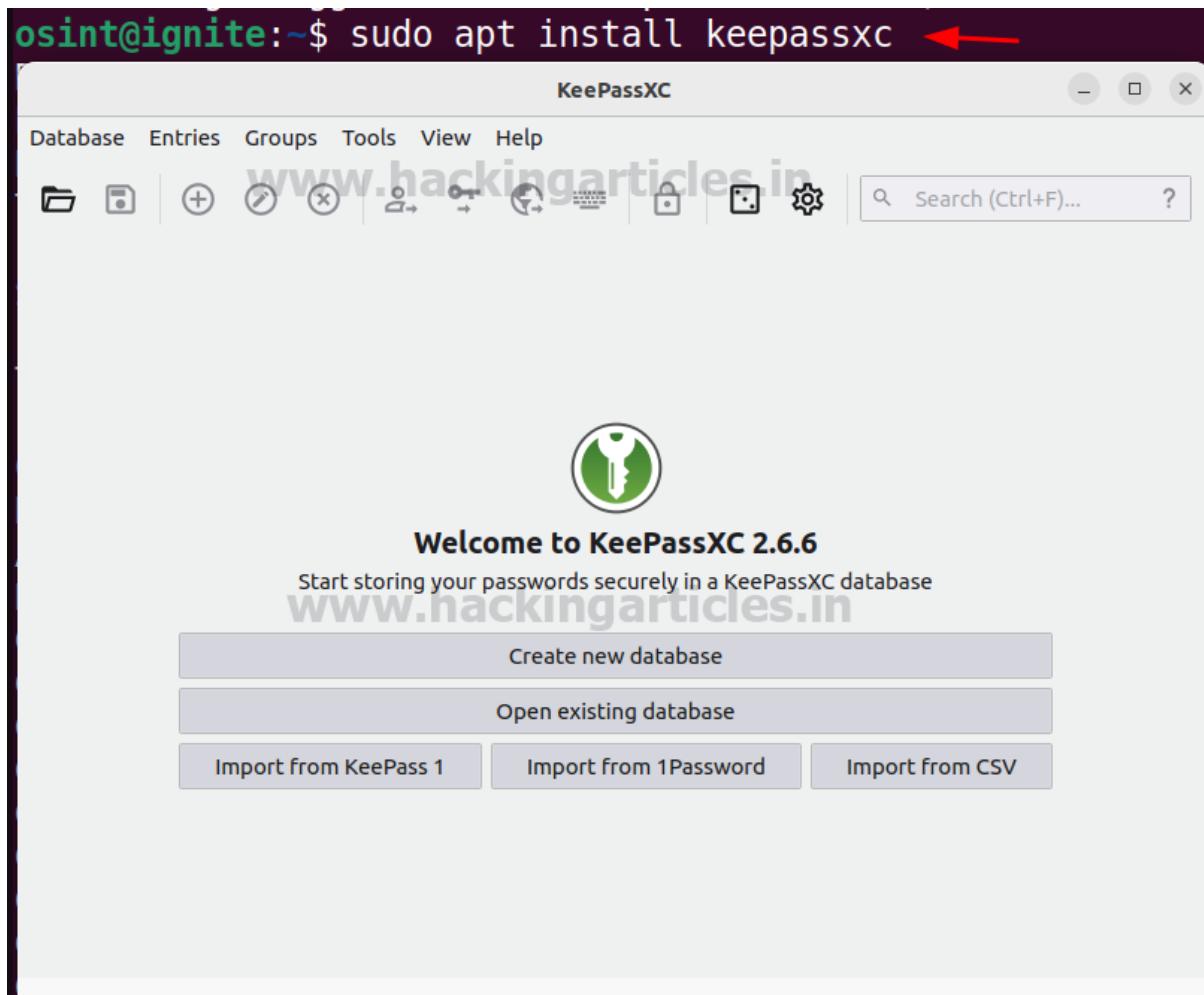


KeePassXC

KeePassXC is an **open-source tool for password management**. It helps users **securely store and manage** their passwords and sensitive information. Therefore, it plays a crucial role in maintaining **Linux telemetry and privacy**.

Installation of KeePassXC can be performed using the following command:

```
sudo apt install keepassxc
```



Virus Scanner

In this section, we will install **ClamAV**, an **open-source antivirus** that **scans** for malware and malicious files. The GUI of **ClamAV** is called **ClamTK**, and to fetch the latest malware detection updates, we must enable **freshclam**.

```
apt install clamav clamav-daemon
apt install clamtk
sudo systemctl stop clamav-freshclam
sudo systemctl enable clamav-freshclam --now
```



```
osint@ignite:~$ sudo apt install clamav clamav-daemon ←
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
clamav is already the newest version (0.103.11+dfsg-0ubuntu0.22.04.1).
clamav-daemon is already the newest version (0.103.11+dfsg-0ubuntu0.22.04.1).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
osint@ignite:~$ sudo apt install clamtk ←
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
clamtk is already the newest version (6.07-1).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
osint@ignite:~$ sudo systemctl stop clamav-freshclam ←
osint@ignite:~$ sudo systemctl enable clamav-freshclam --now ←
Synchronizing state of clamav-freshclam.service with SysV service script with
Executing: /lib/systemd/systemd-sysv-install enable clamav-freshclam
osint@ignite:~$
```



Metadata removal

Sometimes, when transferring files, **metadata** containing **private information** also transfers along with the file. To prevent this, we will use **MAT2 (Metadata Anonymisation Toolkit 2)** to remove **metadata** from files and enhance **privacy**.

To install the MAT2 tool, we can use the following commands:

```
sudo apt install mat2
```

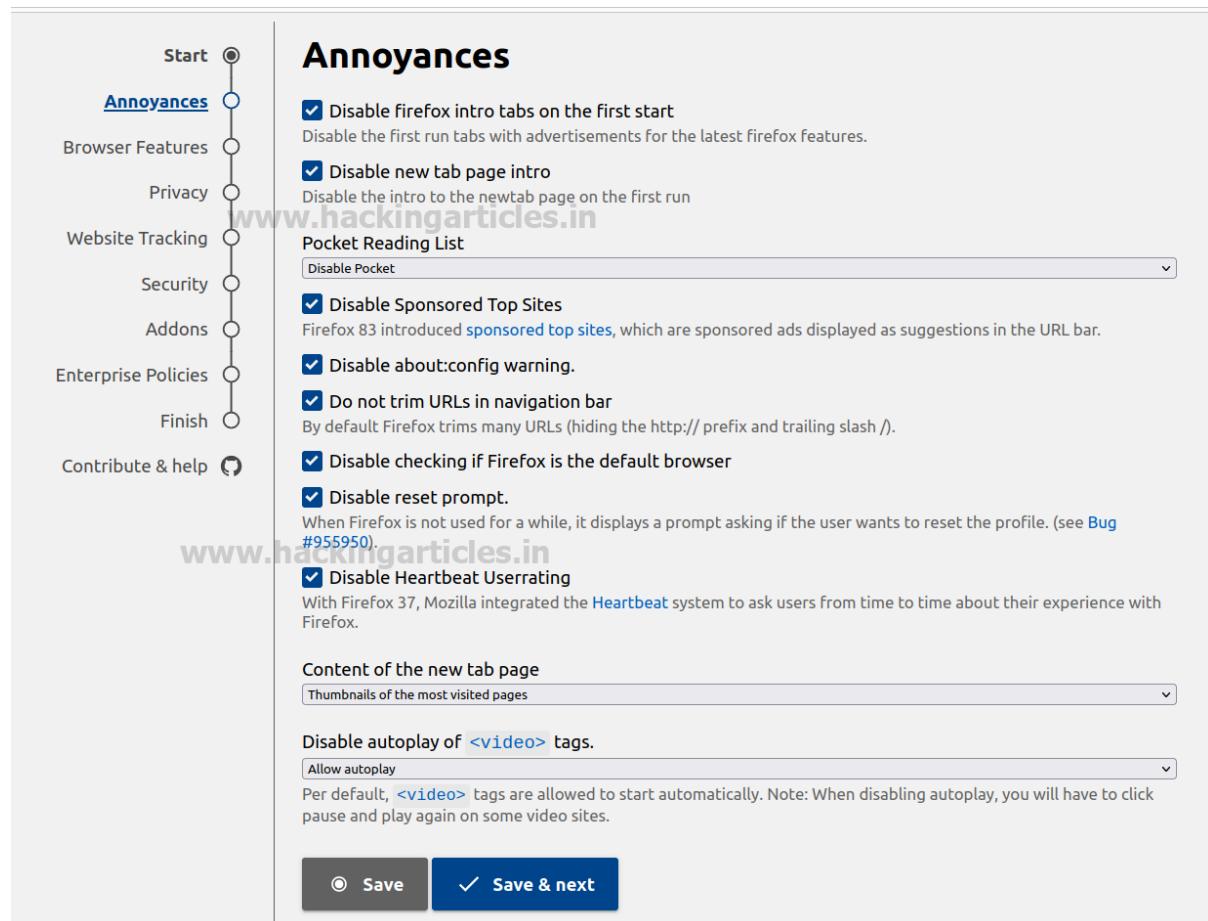
```
osint@ignite:~$ sudo apt install mat2 ←
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed
  gir1.2-nautilus-3.0 gir1.2-poppler-0.18 libarchi
Suggested packages:
  libposix-strptime-perl libencode-hanextra-perl l
The following NEW packages will be installed
```

Firefox profilemaker

To download a customized browser setup tailored to your needs, use **Firefox Profilemaker**. It offers a variety of configurations, which you can set and then download as a **profile** or **preference file**. Finally, you can import it into the browser, ensuring **full customization** and enhancing **Linux telemetry and privacy**.

The profile setup can be performed using the following URL:

<https://ffprofile.com/>



The screenshot shows the Firefox Profilemaker interface. On the left, there's a navigation sidebar with options like Start, Annoyances (which is selected), Browser Features, Privacy, Website Tracking, Security, Addons, Enterprise Policies, and Finish. Below the sidebar, there's a 'Contribute & help' link. The main content area is titled 'Annoyances'. It contains several configuration sections with checkboxes and descriptions. Some sections include dropdown menus for selecting options. At the bottom, there are two buttons: 'Save' and 'Save & next'.

Annoyances

- Disable Firefox intro tabs on the first start
Disable the first run tabs with advertisements for the latest Firefox features.
- Disable new tab page intro
Disable the intro to the newtab page on the first run
- Pocket Reading List**
- Disable Sponsored Top Sites
Firefox 83 introduced [sponsored top sites](#), which are sponsored ads displayed as suggestions in the URL bar.
- Disable about:config warning.
- Do not trim URLs in navigation bar
By default Firefox trims many URLs (hiding the http:// prefix and trailing slash /).
- Disable checking if Firefox is the default browser
- Disable reset prompt.
When Firefox is not used for a while, it displays a prompt asking if the user wants to reset the profile. (see [Bug #955950](#))
- Disable Heartbeat Userrating
With Firefox 37, Mozilla integrated the [Heartbeat](#) system to ask users from time to time about their experience with Firefox.

Content of the new tab page

Disable autoplay of <video> tags.

Per default, <video> tags are allowed to start automatically. Note: When disabling autoplay, you will have to click pause and play again on some video sites.

Save Save & next



Flatpak

Flatpak installs and runs applications within a sandboxed environment. Applications installed via Flatpak run in isolation. This prevents apps from interfering with the system or accessing unauthorized resources, increasing security.

Following are the commands to install the flatpak:

```
sudo apt install flatpak
sudo apt install gnome-software-plugin-flatpak
flatpak remote-add --if-not-exists flathub https://dl.flathub.org/report/flathub.flatpakrepo
```

```
osint@ignite:~$ sudo apt install flatpak ←
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
flatpak is already the newest version (1.12.7-1).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
osint@ignite:~$ sudo apt install gnome-software-plugin-flatpak ←
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnome-software-plugin-flatpak is already the newest version (41.5-2ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
osint@ignite:~$ flatpak remote-add --if-not-exists flathub https://dl.flathub.org/repo/flathub.flatpakrepo ←

Note that the directories
'/var/lib/flatpak/exports/share'
'/home/osint/.local/share/flatpak/exports/share'

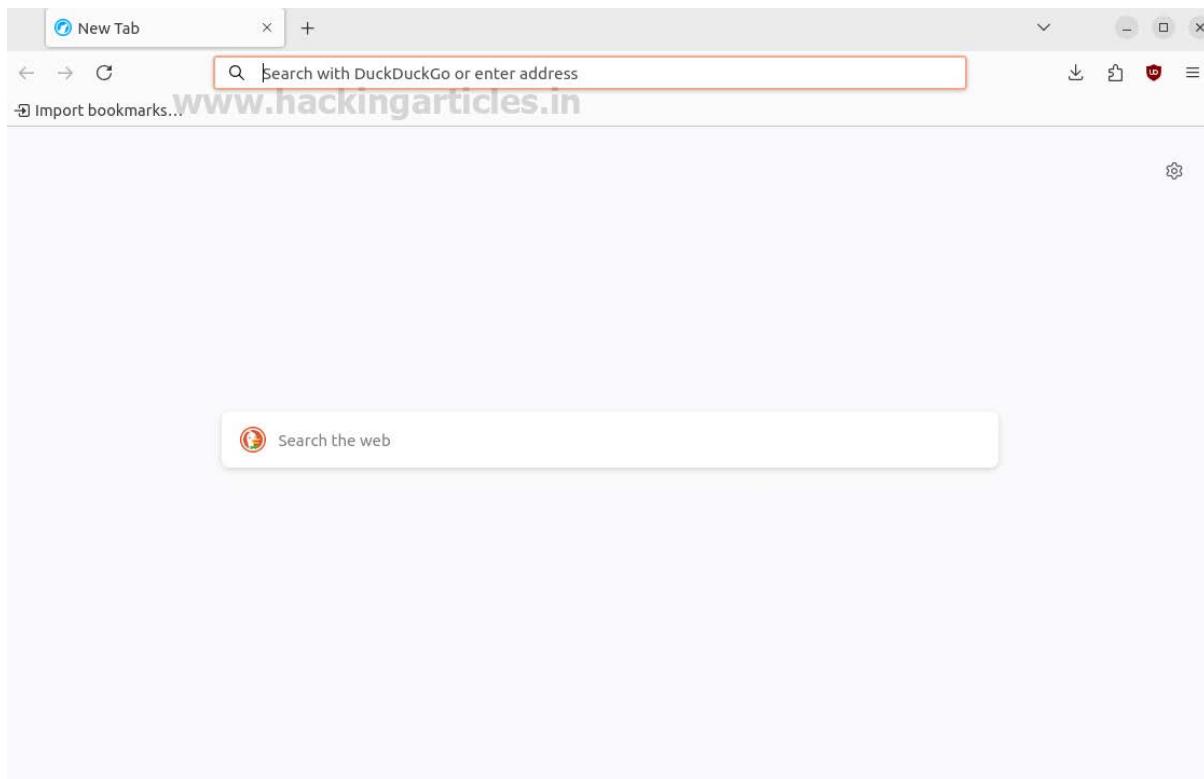
are not in the search path set by the XDG_DATA_DIRS environment variable, so
applications installed by Flatpak may not appear on your desktop until the
session is restarted.
```

LibreWolf

LibreWolf is a web browser focused on privacy; it comes with improved security settings by default. It eliminates **Linux telemetry and privacy** risks, data collection, and tracking features found in standard Firefox, offering a more private browsing experience. By using LibreWolf, users can mitigate issues surrounding **Linux telemetry and privacy** and maintain greater control over their data.

To run the LibreWolf using the flatpack we can use the following command:

```
flatpak run io.gitlab.librewolf-community
```



VeraCrypt

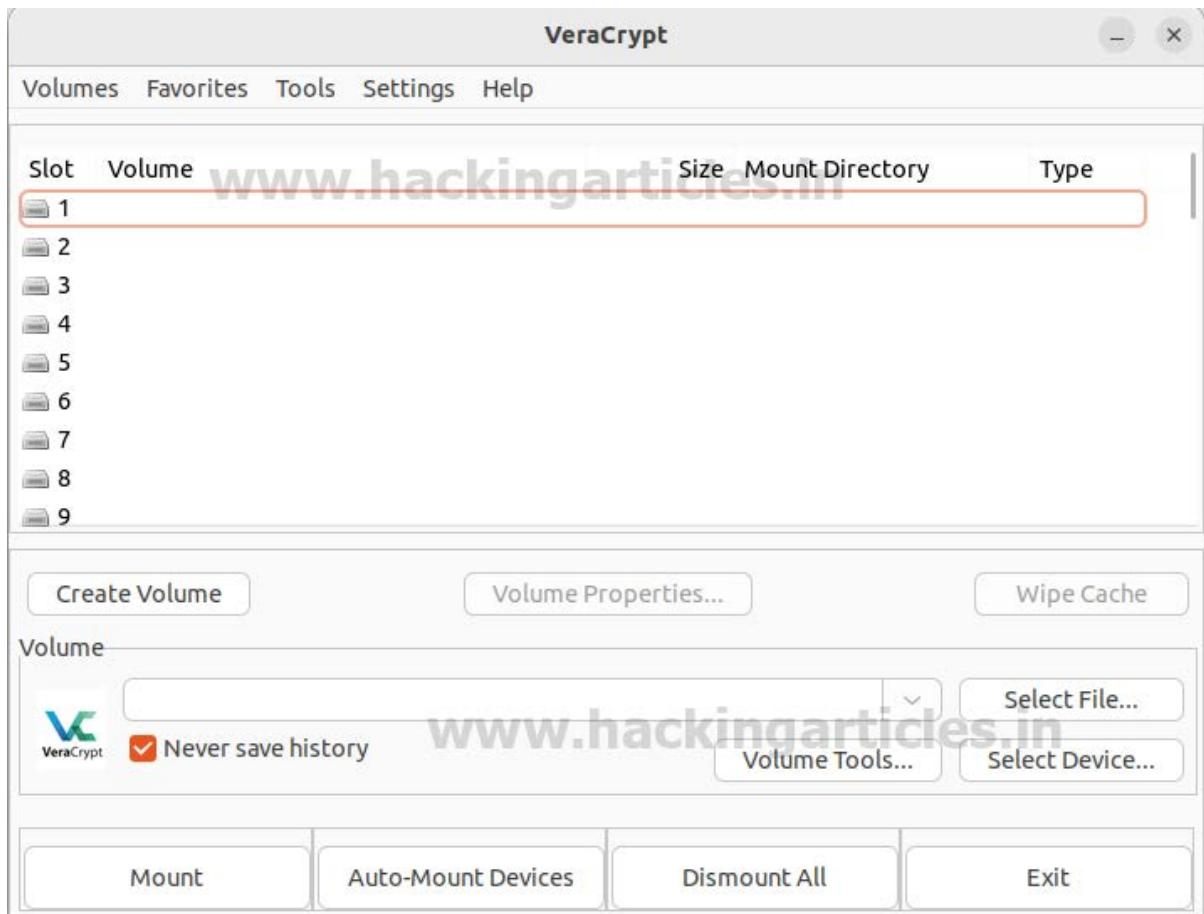
To create a virtual encrypted disk or encrypt the entire partition or storage devices, we can use VeraCrypt. To perform its installation, we need to add the **unit193/encryption** repository in the **PPA (Personal Package Archive)** and then update the system and install VeraCrypt.

```
sudo add-apt-repository ppa:unit193/encryption -y  
sudo apt update  
sudo apt install veracrypt
```



```
osint@ignite:~$ sudo add-apt-repository ppa:unit193/encryption -y ←  
[sudo] password for osint:  
F  
R  
D  
h  
V  
D  
M  
A  
A  
A  
H  
H  
H  
H  
G  
G  
C  
Fetched 25.7 kB in 2s (12.4 kB/s)  
Reading package lists... Done  
osint@ignite:~$  
osint@ignite:~$ sudo apt update ←  
H  
H  
H  
H  
H  
R  
E  
Reading state information... done  
3 packages can be upgraded. Run 'apt list --upgradable' to see them.  
osint@ignite:~$ sudo apt install veracrypt ←  
R  
B  
R  
T  
T  
C
```

After installation we can launch the VeraCrypt.



Tor Browser

To maintain complete anonymity, Tor browser is an amazing browser to search for things. It directs the traffic through the Tor network making it difficult to track.

It can be downloaded from the following website:

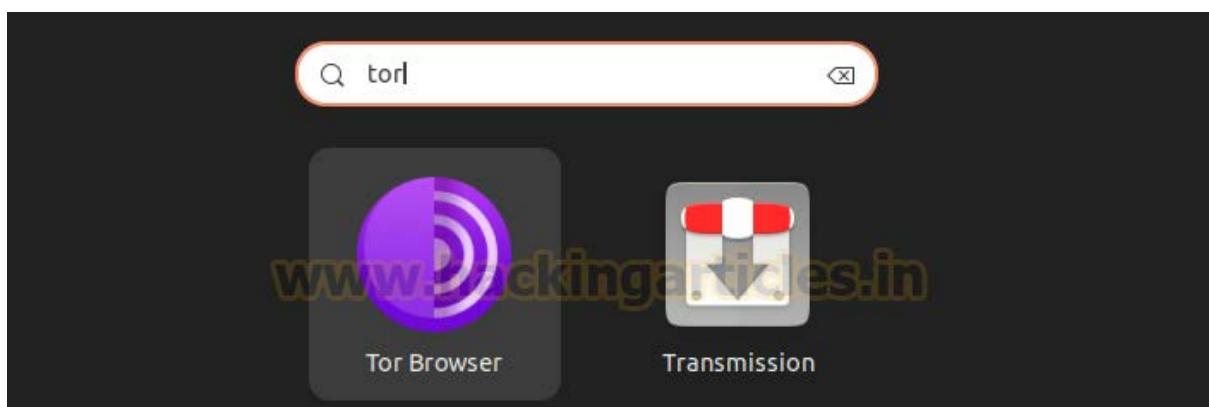
<https://www.torproject.org/download/>



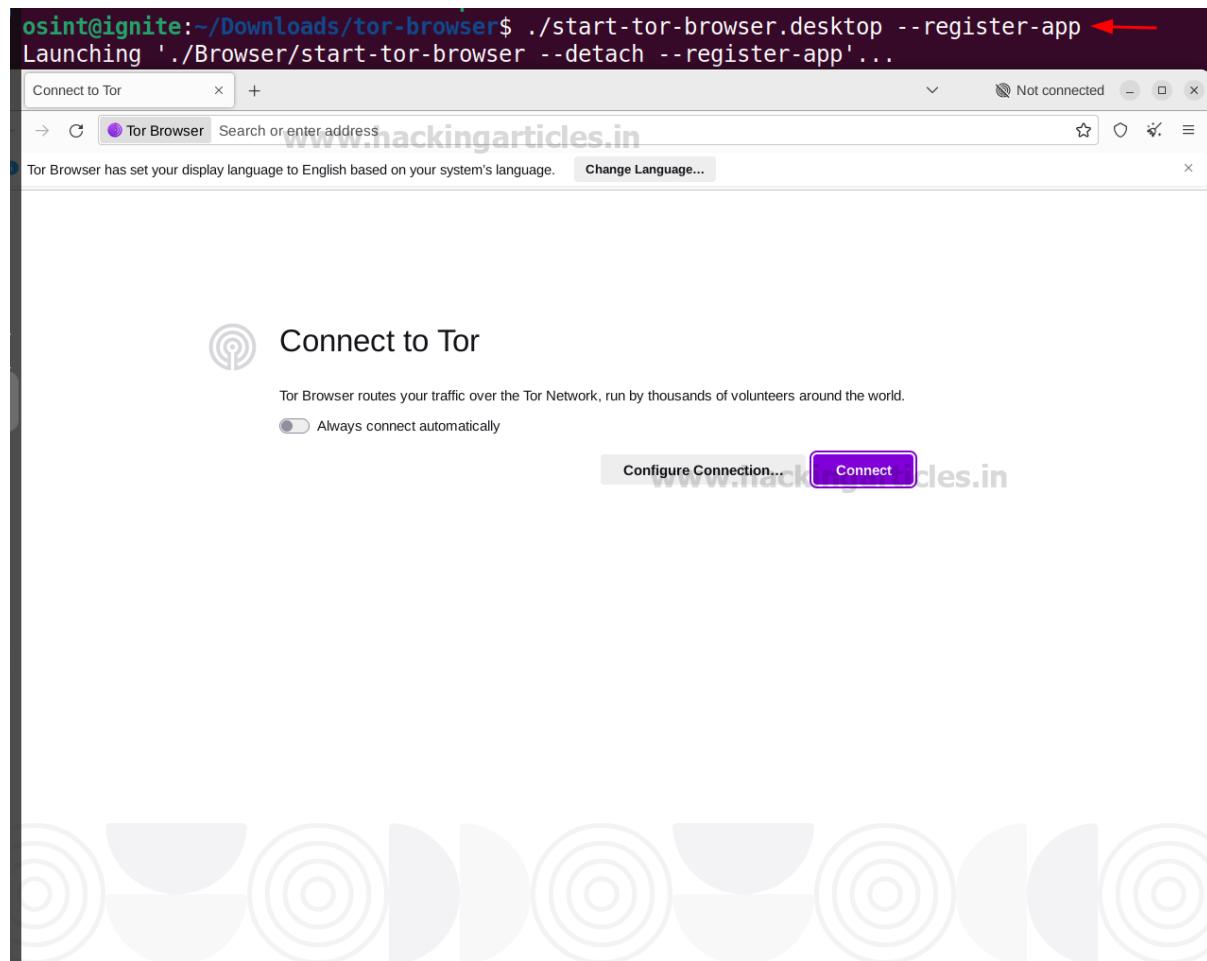
The screenshot shows the official Tor Project download page. At the top, there's a navigation bar with links for 'Donate Now', 'About', 'Support', 'Community', 'Blog', 'Donate', and language selection ('English (en)'). Below the navigation is a large heading 'Download Tor Browser' and a subtext 'Protect yourself against tracking, surveillance, and censorship.' Below this, there are four download options: 'Download for Windows', 'Download for macOS', 'Download for Linux' (which is highlighted with a red box), and 'Download for Android'. Each option includes a 'Signature' link below it. At the bottom of the main section are links for 'Download for another platform', 'Download the latest alpha build', and 'Download Tor'. A smaller screenshot of the Tor Browser window is shown at the bottom, with the search bar containing 'tor'.

After downloading, extract the file and start the browser. Use the `--register-app` flag to launch the Tor browser from the applications menu.

```
./start-tor-browser.desktop --register-app
```



After successful installation, the browser can be launched from the applications menu.



Proton VPN

Proton VPN is a widely used VPN which gives 3 locations as a free service. It helps to remain anonymous and perform the tasks. It can be downloaded from the following link:
<https://protonvpn.com/support/official-linux-vpn-debian/>

Following are the steps to install the Proton VPN:

```
sudo wget https://repo.protonvpn.com/debian/dists/stable/main/binary-all/protonvpn-stable-release_1.0.4_all.deb
```



```
sudo dpkg -i ./protonvpn-stable-release_1.0.4_all.deb && sudo apt update
```



```
osint@ignite:~$ sudo dpkg -i ./protonvpn-stable-release_1.0.4_all.deb && sudo apt update ←
Selecting previously unselected package protonvpn-stable-release.
(Reading database ... 207688 files and directories currently installed.)
Preparing to unpack .../protonvpn-stable-release_1.0.4_all.deb ...
Unpacking protonvpn-stable-release (1.0.4) ...
Setting up protonvpn-stable-release (1.0.4) ...
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:4 https://repo.protonvpn.com/debian stable InRelease [2,967 B]
Get:5 https://repo.protonvpn.com/debian stable/main all Packages [120 kB]
```

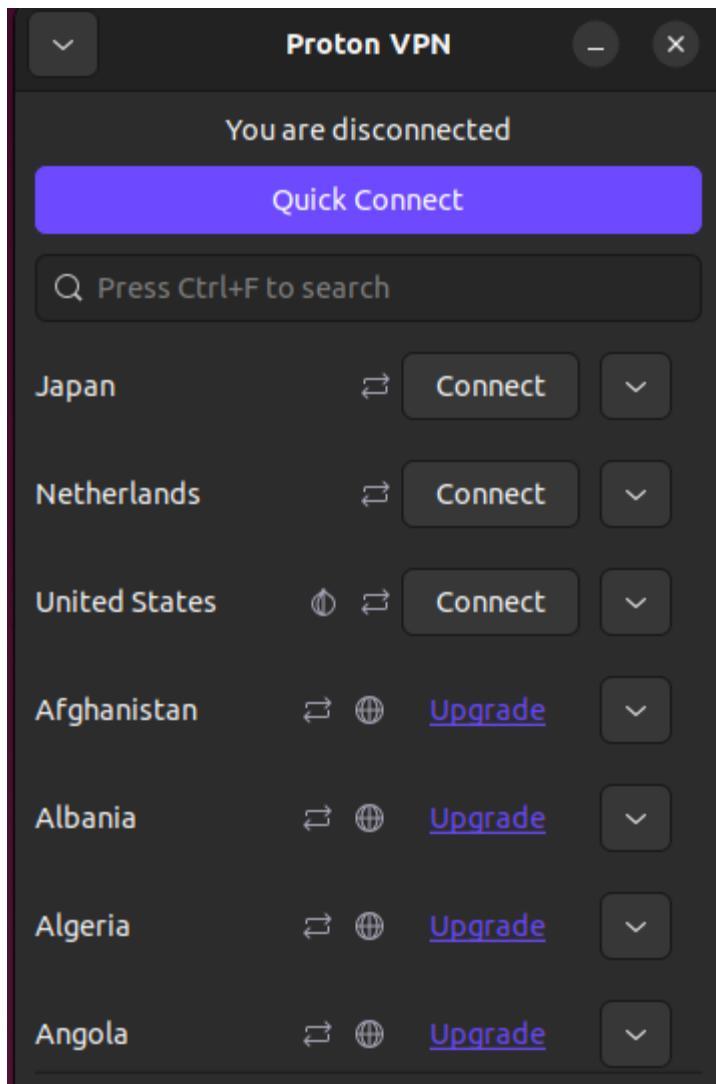
```
echo "62a9d849835de8a5664cf95329458bf1966780b15cec420bf707b5f7278b9027 protonvpn-stable-
release_1.0.4_all.deb" | sha256sum --check -
```

```
osint@ignite:~$ echo "62a9d849835de8a5664cf95329458bf1966780b15cec420bf707b5f7278b9027 protonvpn-stable-release_1.0.4_all.deb" | sha256sum --check -
```

```
sudo apt update && sudo apt upgrade
sudo apt install proton-vpn-gnome-desktop
```

```
osint@ignite:~$ sudo apt update && sudo apt upgrade ←
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 https://repo.protonvpn.com/debian stable InRelease
Hit:5 https://ppa.launchpadcontent.net/unit193/encryption/ubuntu InRelease
Hit:6 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
osint@ignite:~$ sudo apt install proton-vpn-gnome-desktop ←
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  javascript-common libjs-jquery proton-vpn-gtk-app python-babel-
  python3-openssl python3-packaging python3-proton-core python3-p
  python3-proton-vpn-local-agent python3-proton-vpn-logger python
Suggested packages:
  apache2 | lighttpd | httpd gir1.2-ayatanaappindicator3-0.1 python3-p
The following NEW packages will be installed:
```

After the installation is complete, we can launch the Proton VPN.



After connecting with the Netherlands location, we can check the public IP.



The screenshot shows a web browser window with the URL <https://www.dnsleaktest.com>. The page displays the text "Hello 169.150.196.84" in large bold letters, followed by "from Amsterdam, Netherlands" and the Dutch flag. Below this, there are two buttons: "Standard test" and "Extended test", with a link "Whats the difference?" underneath. At the bottom of the page, there is a small footer with the text "Privacy policy | IVPN Limited 2024".

NextDNS

NextDNS is a cloud-based DNS solution which helps to perform content filtering and many more things. It serves as an alternative to the DNS provided by the ISP. Sometimes, we want to block access to certain websites in our system and check which websites the user visited.

The profile can be setup using the DNS address given at the following link:

<https://my.nextdns.io/2f7664/setup>



NextDNS My First Profile ▾

Setup Security Privacy Parental Control Denylist Allowlist Analytics Logs
Settings

- This device is using NextDNS with another profile.
Make sure you are using one of the endpoints listed on this page.

www.hackingarticles.in

Endpoints

Set up NextDNS with this profile using one of the endpoints below.

ID	1772ce
DNS-over-TLS/QUIC	1772ce.dns.nextdns.io
DNS-over-HTTPS	https://dns.nextdns.io/1772ce
IPv6	2a07:a8c0::17:72ce 2a07:a8c1::17:72ce

Not sure how to use those? Follow the [Setup Guide](#).

Linked IP

If you are unable to set up NextDNS using our apps, DNS-over-TLS, DNS-over-HTTPS or IPv6, then use the DNS servers below and link your IP. This is mostly for use on home networks and not recommended on mobile.

DNS Servers	45.90.28.244
	45.90.30.244

Linked IP

[Link IP](#)

[Show advanced options](#) ▾

Setup Guide

Follow the instructions below to set up NextDNS on your device, browser or router.

Android iOS Windows macOS Linux ChromeOS Browsers

Routers

www.hackingarticles.in

RECOMMENDED

systemd-resolved

Use the following in /etc/systemd/resolved.conf:

```
[Resolve]
DNS=45.90.28.0#1772ce.dns.nextdns.io
DNS=2a07:a8c0::1772ce.dns.nextdns.io
DNS=45.90.30.0#1772ce.dns.nextdns.io
DNS=2a07:a8c1::1772ce.dns.nextdns.io
DNSOverTLS=yes
```

After copying the systemd-resolved addresses, we can add this in the /etc/systemd/resolved.conf file.

```
sudo nano /etc/systemd/resolved.conf
cat /etc/systemd/resolved.conf
```



```
osint@ignite:~$ sudo nano /etc/systemd/resolved.conf ←
osint@ignite:~$ cat /etc/systemd/resolved.conf
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or
# terms of the GNU Lesser General Public License as published
# Software Foundation; either version 2.1 of the License, or
# any later version. www.hackingarticles.in
#
# Entries in this file show the compile time defaults. Local
# should be created by either modifying this file, or by creating
# the resolved.conf.d/ subdirectory. The latter is generally
# Defaults can be restored by simply deleting this file and
#
# Use 'systemd-analyze cat-config systemd/resolved.conf' to
#
# See resolved.conf(5) for details.

[Resolve]
# Some examples of DNS servers which may be used for DNS=
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-
# Google:      8.8.8.8#dns.google 8.8.4.4#dns.google 2001:486
# Quad9:       9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9
#DNS=
#FallbackDNS=
#Domains=
#DNSSEC=no
#DNSOverTLS=no
#MulticastDNS=no
#LLMNR=no
#Cache=no-negative
#CacheFromLocalhost=no
#DNSStubListener=yes
#DNSStubListenerExtra=
#ReadEtcHosts=yes
#ResolveUnicastSingleLabel=no
[Resolve]
DNS=45.90.28.0#1772ce.dns.nextdns.io
DNS=2a07:a8c0::#1772ce.dns.nextdns.io
DNS=45.90.30.0#1772ce.dns.nextdns.io
DNS=2a07:a8c1::#1772ce.dns.nextdns.io
DNSOverTLS=yes
osint@ignite:~$
```



After adding the addresses to the configuration file, navigate to Settings in the browser and select DNS over HTTPS. It should be set to Max Protection. Inside Max Protection select the custom DNS and enter the NextDNS URL shown in the DNS over HTTPS.

DNS over HTTPS

Domain Name System (DNS) over HTTPS sends your request for a domain name through an encrypted connection, providing a secure DNS and making it harder for others to see which website you're about to access.

[Learn more](#)

Status: Active [Learn more](#)

Provider: dns.nextdns.io

[Manage Exceptions...](#)

Enable DNS over HTTPS using:

Default Protection

LibreWolf decides when to use secure DNS to protect your privacy.

Increased Protection

You control when to use secure DNS and choose your provider.

Max Protection

LibreWolf will always use secure DNS. You'll see a security risk warning before we use your system DNS.

- Only use the provider you select
- Always warn if secure DNS isn't available
- If secure DNS is not available sites will not load or function properly

Choose provider:

Custom

https://dns.nextdns.io/1772ce|

Off

Use your default DNS resolver

After the configuration is complete, the NextDNS setup will show an All **good!** status.



All good!
This device is using NextDNS with this profile.

We can also restrict websites from visiting by adding them in the **Parental Control** list.

Facebook

The user is no longer able to visit the website.



The screenshot shows a browser window with the LibreWolf logo in the top left. The title bar has tabs for "Parental Control - My Firs" and "Problem loading page". The address bar shows the URL "https://www.facebook.com". The main content area displays an "Unable to connect" error message with the following text:
An error occurred during a connection to www.facebook.com.
• The site could be temporarily unavailable or too busy. Try again in a few moments.
• If you are unable to load any pages, check your computer's network connection.
• If your computer or network is protected by a firewall or proxy, make sure that LibreWolf is permitted to access the web.

[Try Again](#)

There is also a feature to check the logs, which can help in tracking the websites visited before in the **Logs** option.



The screenshot shows the NextDNS web interface with the 'Logs' tab selected. The page title is 'My First Profile ▾'. Other tabs include 'Setup', 'Security', 'Privacy', 'Parental Control', 'Denylist', 'Allowlist', 'Analytics', and 'Logs'. A dropdown menu 'All devices ▾' is open. The main area lists DNS queries with icons for each domain:

- www.facebook.com
- scontent.cdninstagram.com
- static.cdninstagram.com
- www.instagram.com
- external-content.duckduckgo.com
- links.duckduckgo.com
- duckduckgo.com
- www.facebook.com
- my.nextdns.io
- favicons.nextdns.io
- api.nextdns.io
- my.nextdns.io

Conclusion

As we become aware of the effects of **Linux telemetry and privacy**, we can make choices that lead to a safer and more private computing environment. By using the above methods and tools, we can safeguard users' **privacy** and significantly reduce our exposure to unwanted data collection, including **Linux telemetry and privacy** concerns.

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

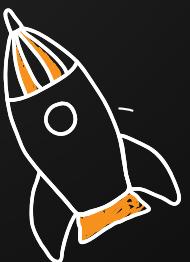
Ethical Hacking

Bug Bounty

Network Security Essentials

Network Pentest

Wireless Pentest



ADVANCED

Burp Suite Pro

Web Services-API

Pro Infrastructure VAPT

Computer Forensics

Android Pentest

Advanced Metasploit

CTF



EXPERT

Red Team Operation

Privilege Escalation

- APT's - MITRE Attack Tactics
- Active Directory Attack
- MSSQL Security Assessment

Windows

Linux

