

Remove viruses from Windows PC with Ubuntu Live USB

Your Windows computer is infected with a virus or worse, you can't even start it. If you own a CD or Ubuntu Live USB, you can use it to clean your PC and try to recover Windows.

Your Windows computer is infected with a virus or worse, you can't even start it. If you own a CD or Ubuntu Live USB, you can use it to clean your PC and try to recover Windows.

Every Microsoft Windows user knows how easily the operating system is vulnerable to malware and viruses. If your Windows PC is infected with a virus, there are several ways to 'clean up' the PC.

If Windows can boot, at least you have the opportunity to launch your favorite antivirus program and start cleaning. But, what if the virus infection is so serious that Windows cannot boot? Your entire private data is at risk.

In this guide, **Quantrimang.com** will show you how to clean your Windows computer from infected viruses by using a CD or Ubuntu Live USB and ClamAV antivirus software. ClamAV is a free and open source antivirus program that can be used on Ubuntu.

If you have a CD or Ubuntu Live USB, you can use it to clean your Windows PC. In case you don't have one, you can create such a tool by following the instructions in the article: [How to create a Live USB or ReactOS CD](#).

Remove viruses from Windows PC with Ubuntu Live USB

Before you begin, make sure that you have changed the BIOS settings on your computer to boot from USB or CD first. Now, start by inserting the Ubuntu Live drive (USB or CD) into the computer and then turning on the power.

Step 1 : When the **Ubuntu Install** window appears, select the '**Try Ubuntu**' option.



Step 2 : When the live Ubuntu session starts successfully, open a terminal and use the following command to update the Ubuntu repository.

```
sudo apt update
```

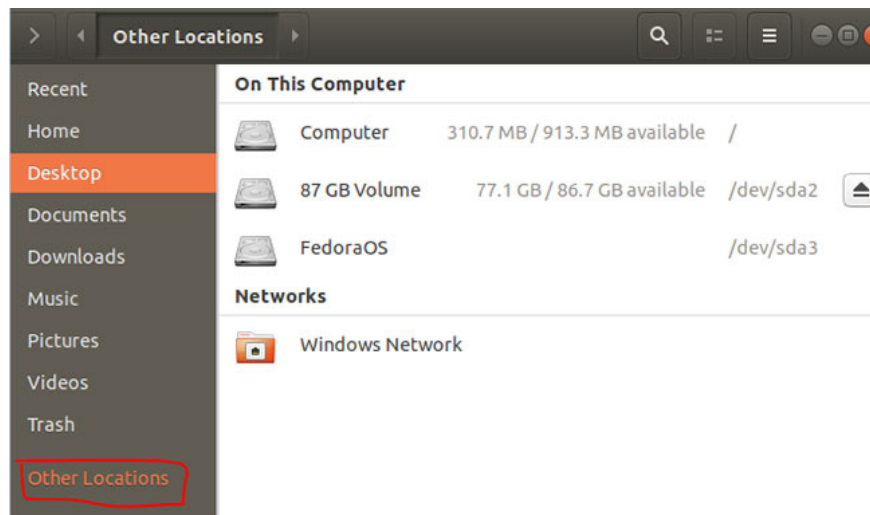
```
ubuntu@ubuntu:~$ sudo apt update
Ign:1 cdrom://Ubuntu 18.04.1 LTS _Bionic Beaver_ - Release amd64
(20180725) bionic InRelease
Hit:2 cdrom://Ubuntu 18.04.1 LTS _Bionic Beaver_ - Release amd64
(20180725) bionic Release
Hit:3 http://archive.ubuntu.com/ubuntu bionic InRelease
Get:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
[88.7 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
[88.7 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/main amd64
Packages [541 kB]
Get:8 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64
Packages [766 kB]
Get:9 http://security.ubuntu.com/ubuntu bionic-security/main
translation-en [180 kB]
```

Step 3 : To install ClamAV antivirus software on Ubuntu, you can use the following command:

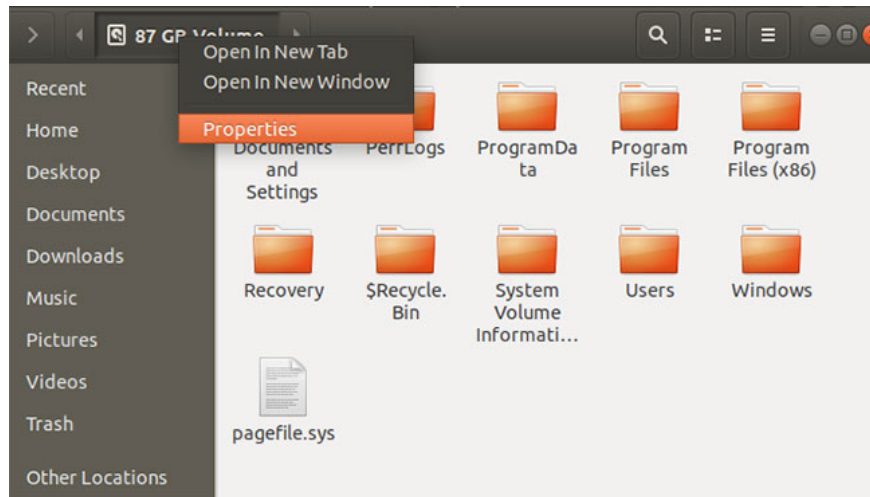
```
sudo apt install clamav
```

```
ubuntu@ubuntu:~$ sudo apt install clamav
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamav-freshclam libclamav7 libcurl4 liblvm3.9
  libmspack0 libtftm1
Suggested packages:
  clamav-docs libclamunrar7
The following NEW packages will be installed:
  clamav clamav-base clamav-freshclam libclamav7 libcurl4
  liblvm3.9 libmspack0 libtftm1
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 12.7 MB of archives.
After this operation, 50.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

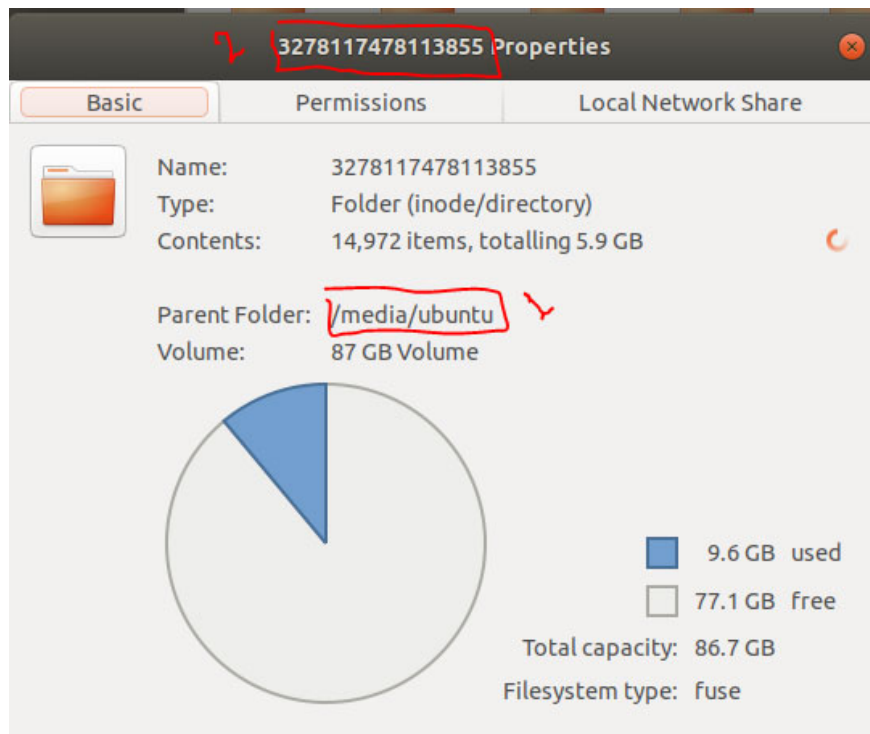
Step 4 : After the ClamAV antivirus software is installed successfully, you need to know the location of the Windows drive to perform the scan. You can find your Windows drive location by opening Ubuntu File Explorer and searching for Windows drive.



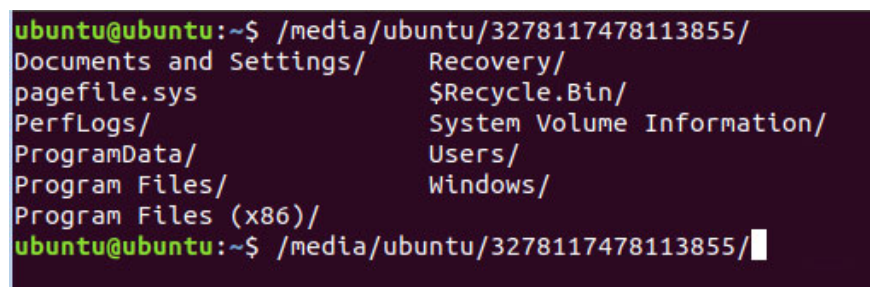
Step 5 : After locating the Windows drive, right-click on the tab named Windows drive from the top panel in File Explorer and select the **Properties** option .



Step 6 : When the **Properties** window opens successfully, get the path and the drive letter from here, as you can see in the screenshot below.



Step 7 : Now go back to the terminal, look for the Windows drive path, as shown in the screenshot below.



Step 8 : Next, you can start scanning your Windows drive with the following command:

```
clamscan -r --bell -i WIN_DRIVE_PATH
```

The previous ClamAV scan command means searching for all infected files and giving notice when found.

```
ubuntu@ubuntu:~$ clamscan -r --bell -i /media/ubuntu/3278117478113855/Users/Hend/Downloads/
----- SCAN SUMMARY -----
Known viruses: 6517347
Engine version: 0.101.4
Scanned directories: 1
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 158.936 sec (2 m 38 s)
ubuntu@ubuntu:~$
```

After the ClamAV scan command finishes successfully, you will get a summary of the scanning process, as you can see in the screenshot above.

Here are some ClamAV scan options:

1. **-r** - Optionally perform recursive scans.
2. **-Exclude = .avi** - The option to exclude a set pattern to skip things like videos or music files.
3. **-Scan-mail = yes / no** - Option to include mail files found during system scan.
4. **-Remove = yes / no** - Option to delete all scanned files or not. Be careful when using this option!

Step 9: To know more about the ClamAV scanning options, use the next command.

```
clamscan --help
```

```
ubuntu@ubuntu:~$ clamscan --help
Clam AntiVirus: Scanner 0.101.4
By The ClamAV Team: https://www.clamav.net/about.html#credits
(C) 2019 Cisco Systems, Inc.

clamscan [options] [file/directory/-]

--help                -h                Show this help
--version             -V                Print version number
--verbose             -v                Be verbose
--archive-verbose     -a                Show filenames inside scanned archives
--debug               -d                Enable libclamav's debug messages
--quiet               -q                Only output error messages
--stdout              -S                Write to stdout instead of stderr
--no-summary          -s                Disable summary at end of scanning
--infected             -i                Only print infected files
--suppress-ok-results -o                Skip printing OK files
--bell                -b                Sound bell on virus detection

--tempdir=DIRECTORY  -T                Create temporary files in DIRECTORY
--leave-temps[=yes/no(*)]
--gen-json[=yes/no(*)]
Generate JSON description of scanned file(s). JSON will be printed and also-
```

Hope you enjoy cleaning up your Windows system with Ubuntu Live USB.

Hope you are succesful.

You finished reading the article "**Remove viruses from Windows PC with Ubuntu Live USB**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
