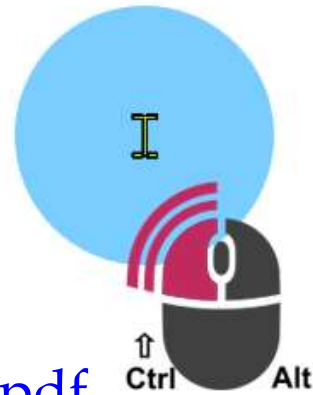




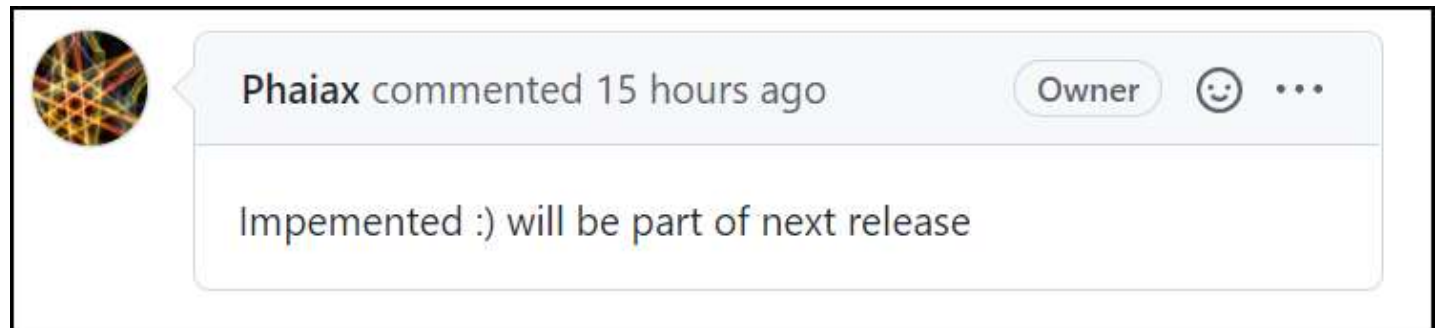
**Alan German & Chris Taylor**  
**Ottawa PC Users' Group**

## Follow-up

# Don't like something? Say something!



- Key-n-Stroke
  - highlights mouse pointer
  - [https://opcug.ca/qa\\_recordings/20211222\\_PowerPoint.pdf](https://opcug.ca/qa_recordings/20211222_PowerPoint.pdf)
- Wish list
  - hide circle for “Indicate cursor position” when mouse pointer disappears (e.g. when watching a YouTube video)
  - add user-definable hot-keys to toggle on/off "Indicate cursor position" & "Show icons on click"
  - submitted to the GitHub project
- 2022-02-04



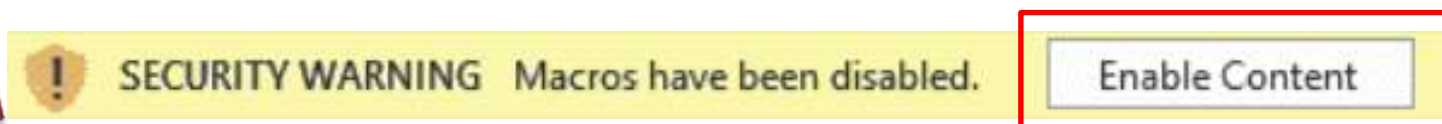
- Bottom line
  - if you want something changed
  - you have to say something!

Share

# Office to block VBA macros

- Visual Basic for Applications (VBA)
  - VBA macros can automate things (a **good** thing)
  - VBA macros can automate malicious things (a **bad** thing)
- Microsoft to block VBA macros starting April 2022
  - in files that came from the Internet

Current



Upcoming



- Work-around
  - save file to disk
  - right-click file, choose *Properties*
  - *General* tab, select *Unblock* checkbox, click OK.

<https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805>

Share

# SmartApps

- Useful apps for Android smartphones and tablets
- What are your favourites?



[SuggestionBox@opcug.ca](mailto:SuggestionBox@opcug.ca)

*Can also be a program for the PC*



# rShopping List for Groceries



- Comes with big list of items
- Add more or change.
- You can set up stores
- Aisles items are on in them
- Get automatic price comparisons and calculations
- Much more (but I only use the basics)

[https://play.google.com/store/apps/  
details?id=com.RayDarLLC.rShopping](https://play.google.com/store/apps/details?id=com.RayDarLLC.rShopping)

Stewart on



Android

# GasBuddy



- A user-generated fuel and gas station reporting service
- Wikipedia for the internal combustion crowd!
- Earn points for reporting prices
- Use them to enter giveaways for fuel



- Unless you live in Quebec... 😞

<https://play.google.com/store/apps/details?id=gbis.gbandroid>

# Preparing to abandon <sup>the windows</sup> ~~ship~~

To-do list:

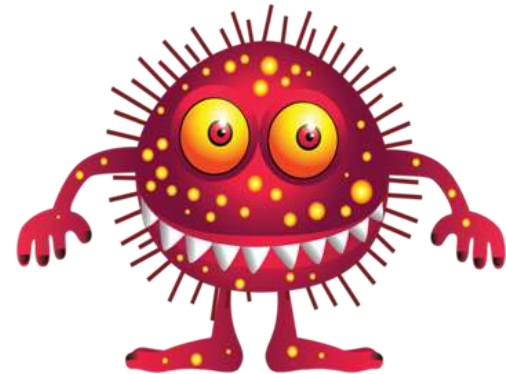
- ✓ (1) Install Linux on the last remaining computer
- ✓ (2) Identify the current uses of Windows 10
- ✓ (3) Identify Linux-based alternatives
- ✓ (4) Find workarounds if alternatives exist

What else do we need to know?

# Linux Security

## Anti-virus

Not installed by default



## Firewall

Installed but not activated

# Why You Don't Need an Antivirus On Linux (Usually)



CHRIS HOFFMAN  @chrisbhoffman

UPDATED JUL 11, 2017, 10:55 PM EST | 3 MIN READ

- Few Linux Viruses Exist in the Wild
- Limited market share (smaller target)
- More computer-literate users (geeks!)
- Limited (non-root) user accounts
- Applications downloaded using Package Managers and Software Repositories
- Background security systems (AppArmor/SELinux)
- AV recommended for mail servers (users sharing Windows file attachments)

<https://www.howtogeek.com/135392/htg-explains-why-you-dont-need-an-antivirus-on-linux-and-when-you-do/>

# Linux-Targeted Malware Increases by 35% in 2021: XorDDoS, Mirai and Mozi Most Prevalent

January 13, 2022 Mihai Maganu Endpoint & Cloud Security



## CATEGORIES

-  Endpoint & Cloud Security
-  Engineering & Tech
-  Executive Viewpoint
-  From The Front Lines
-  Identity Protection
-  Observability & Log Manager
-  People & Culture
-  Remote Workplace
-  Research & Threat Intel
-  Tech Center

<https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/>

# Linux-Targeted Malware Increases by 35% in 2021: XorDDoS, Mirai and Mozi Most Prevalent

January 13, 2022 Mihai Maganu Endpoint & Cloud Security

## CATEGORIES

 Endpoint & Cloud Security

 Engineering & Tech

 Executive Viewpoint

 People & Culture

 Remote Workplace

 Research & Threat Intel

 Tech Center

...targeting Linux-based operating systems, commonly deployed in Internet of Things (IoT) devices...

<https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/>

## Update Manager

File Edit View Help



Clear



Select All



Refresh



Install Updates

| Type | Upgrade | Name                                                                                          | New version         |
|------|---------|-----------------------------------------------------------------------------------------------|---------------------|
|      |         | <b>wget</b><br>Retrieves files from the web                                                   | 1.19.4-1ubuntu2.1   |
|      |         | <b>xdg-utils</b><br>Desktop integration utilities from freedesktop.org                        | 1.1.2-1ubuntu2.2    |
|      |         | <b>Linux kernel 4.15.0.22.23</b><br>The Linux kernel                                          | 4.15.0.22.23        |
|      |         | <b>apturl</b><br>Install packages using the apt protocol - GTK+ frontend                      | 0.5.2+linuxmint7    |
|      |         | <b>blueberry</b><br>A configuration tool for Bluetooth                                        | 1.2.1               |
|      |         | <b>xed</b><br>Text editor                                                                     | 1.8.1+tara          |
|      |         | <b>xplayer</b><br>Media player                                                                | 1.8.1+tara          |
|      |         | <b>xreader</b><br>Document viewer                                                             | 1.8.2+tara          |
|      |         | <b>xviewer</b><br>Image viewer                                                                | 1.8.1+tara          |
|      |         | <b>code</b><br>Code editing. Redefined                                                        | 1.23.1-1525968403   |
|      |         | <b>docker-ce</b><br>Docker: the open-source application container engine                      | 18.03.1~ce-0~ubuntu |
|      |         | <b>sublime-text</b><br>Sublime Text is a sophisticated text editor for code, markup and prose | 3176                |

**Security update****Kernel update****Software update****Third-party update**

Description

Changelog

27 updates selected (294MB)



ClamAV® is an open-source antivirus engine for detecting trojans, viruses, malware & other malicious threats.

download



The latest stable release is version 0.104.1.

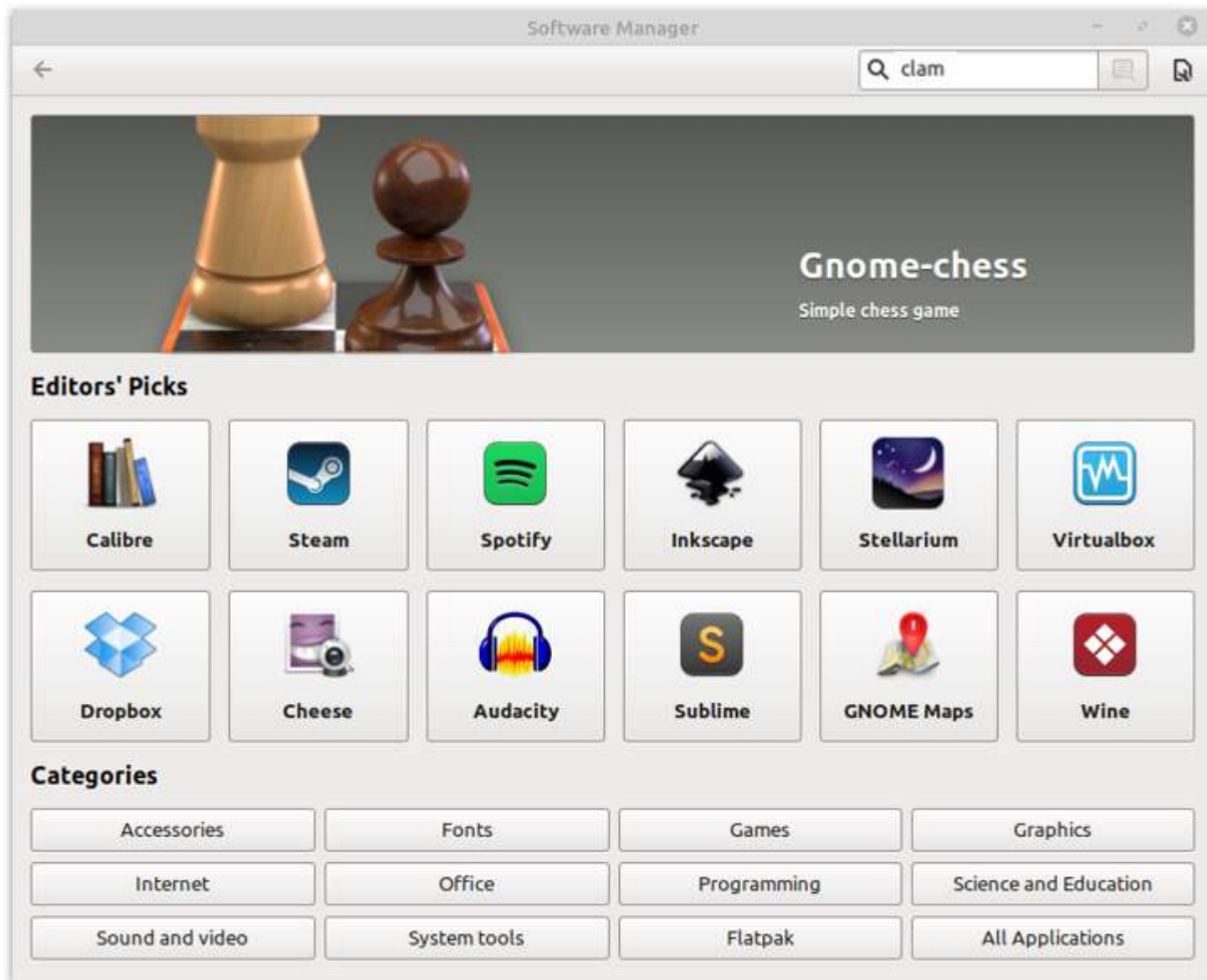
## The Standard

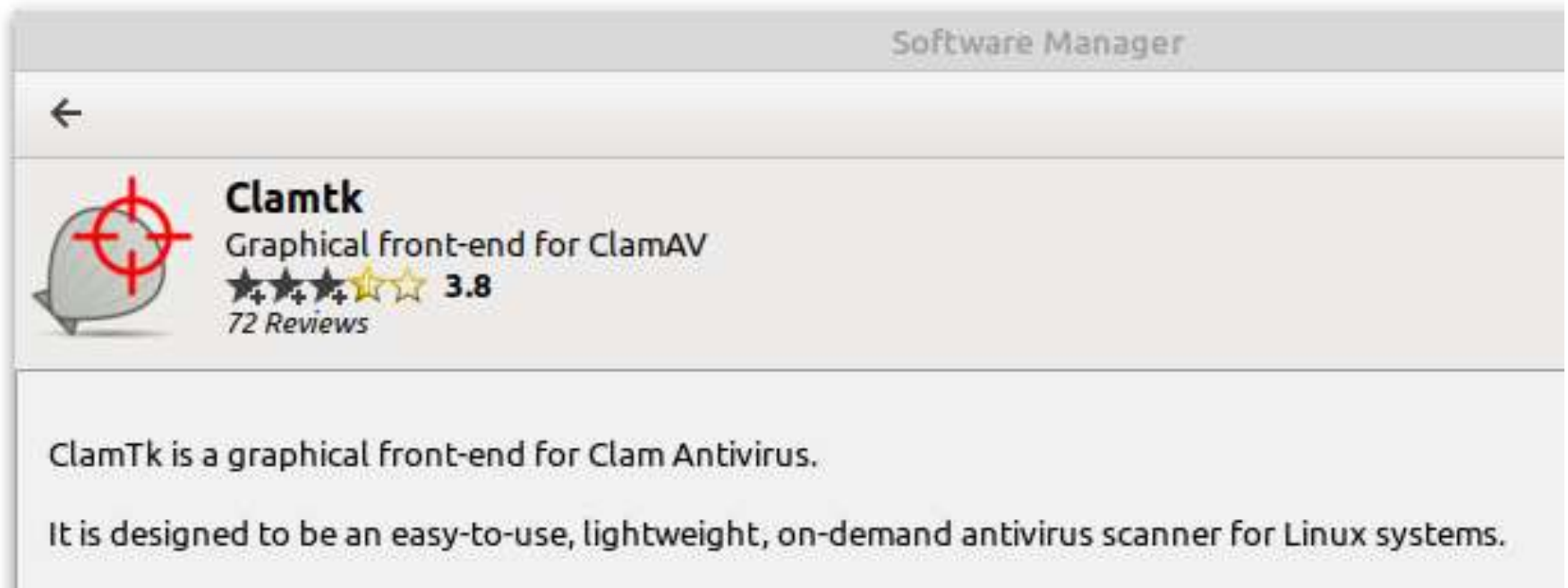
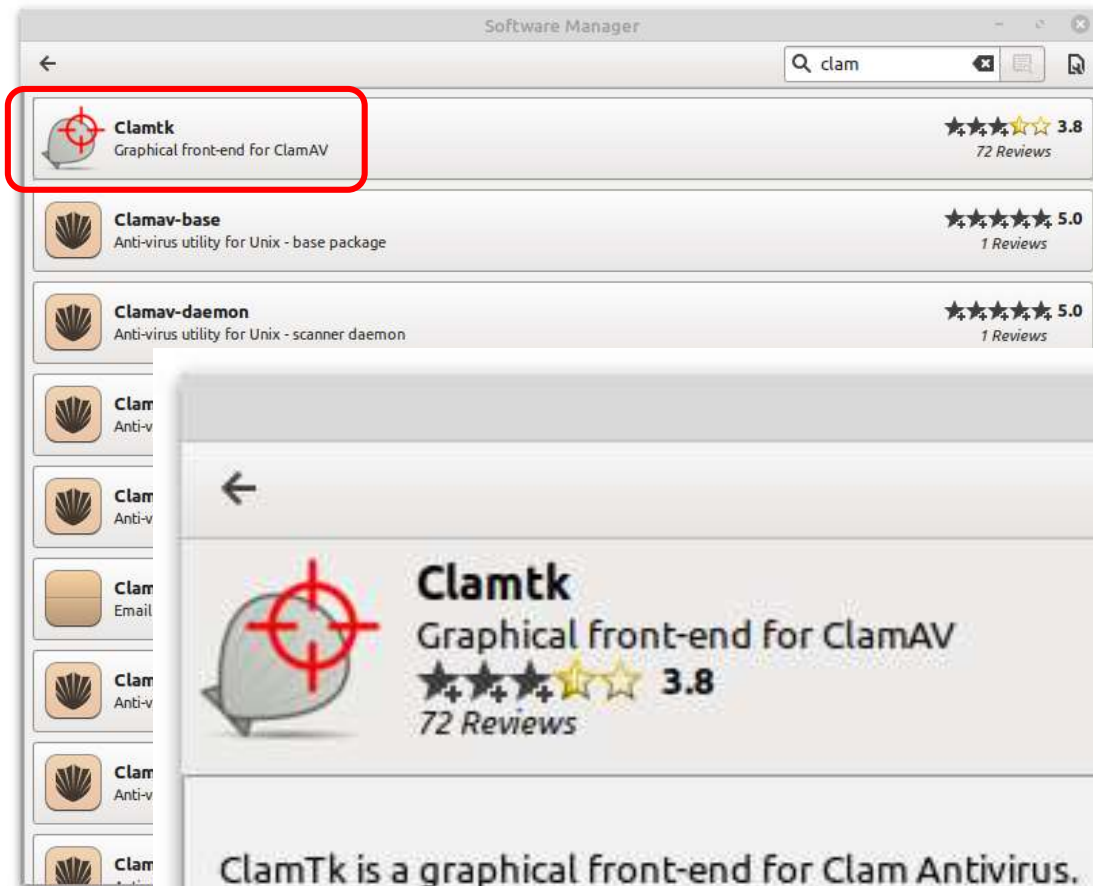
ClamAV® is the open-source standard for mail gateway-scanning software.

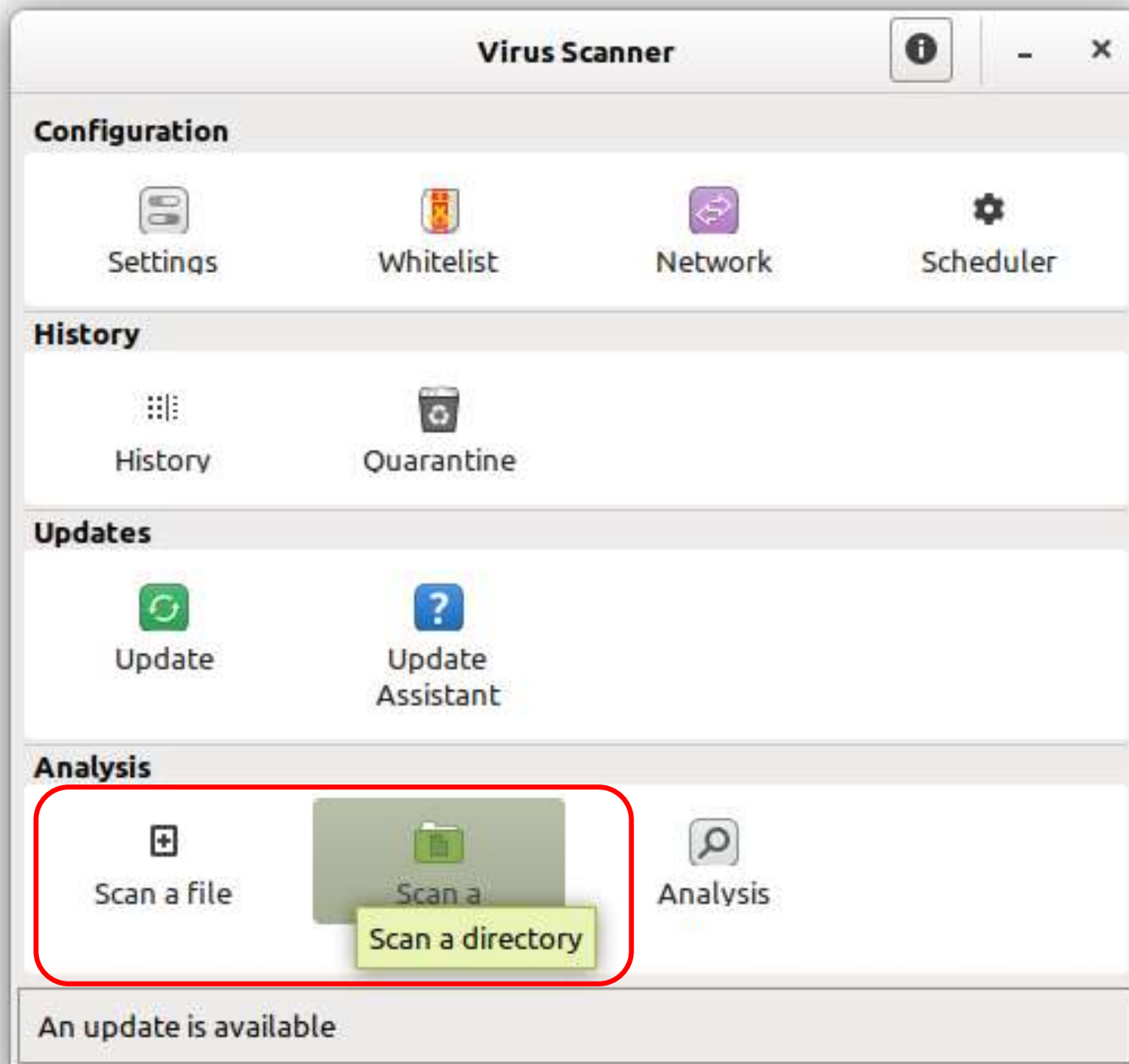
<https://www.clamav.net>

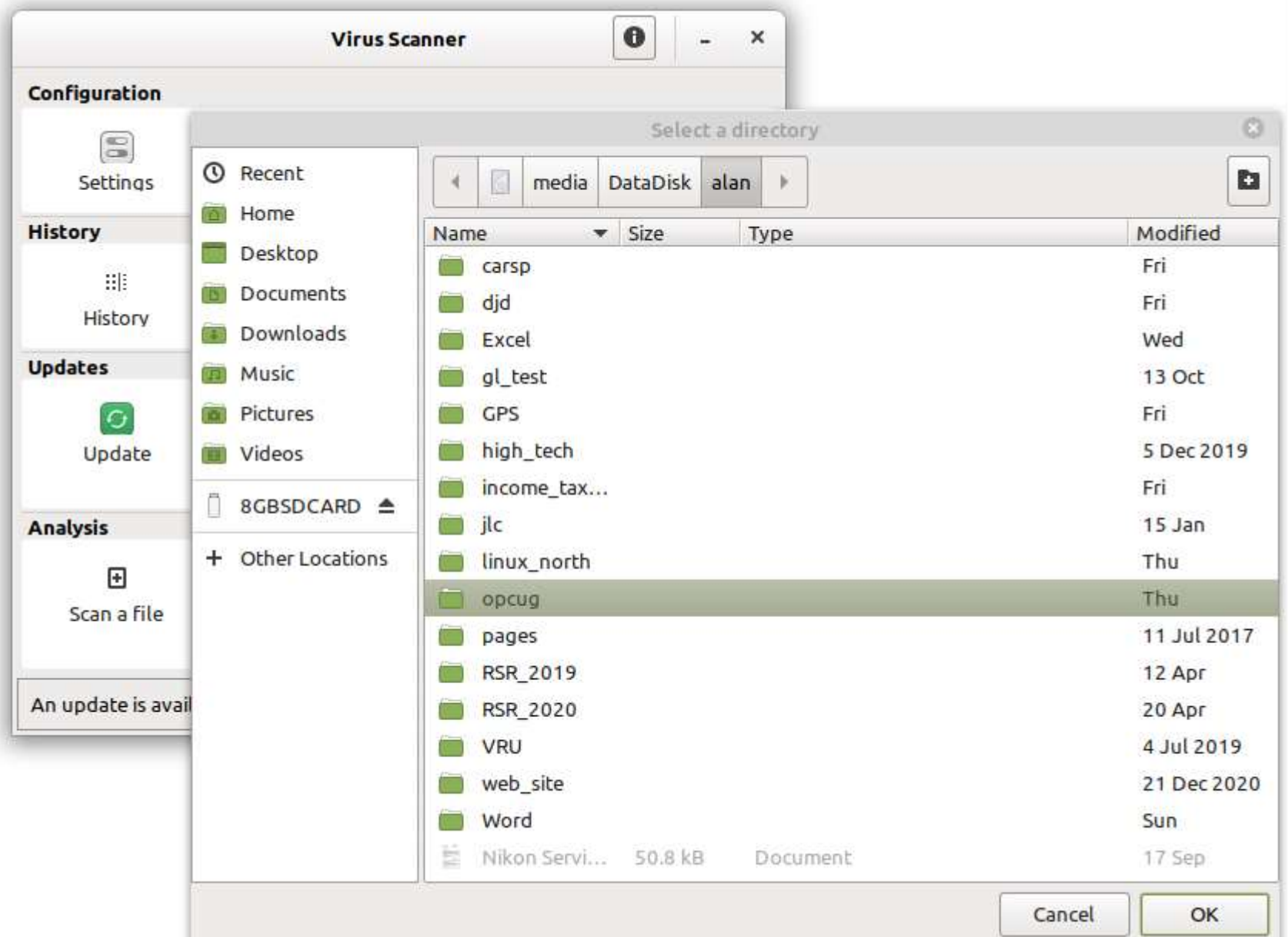
- Open-source (GPL)
- Email, web scanning, and endpoint security
- Flexible and scalable multi-threaded daemon
- ClamOnAcc client for the ClamD scanning daemon provides on-access scanning
- Command-line scanner
- Advanced tool for automatic database updates
- Virus database updated multiple times per day.
- Built-in support for various archive formats including ZIP, Tar, GZIP
- “ClamAV brought to you by Cisco Systems, Inc.”

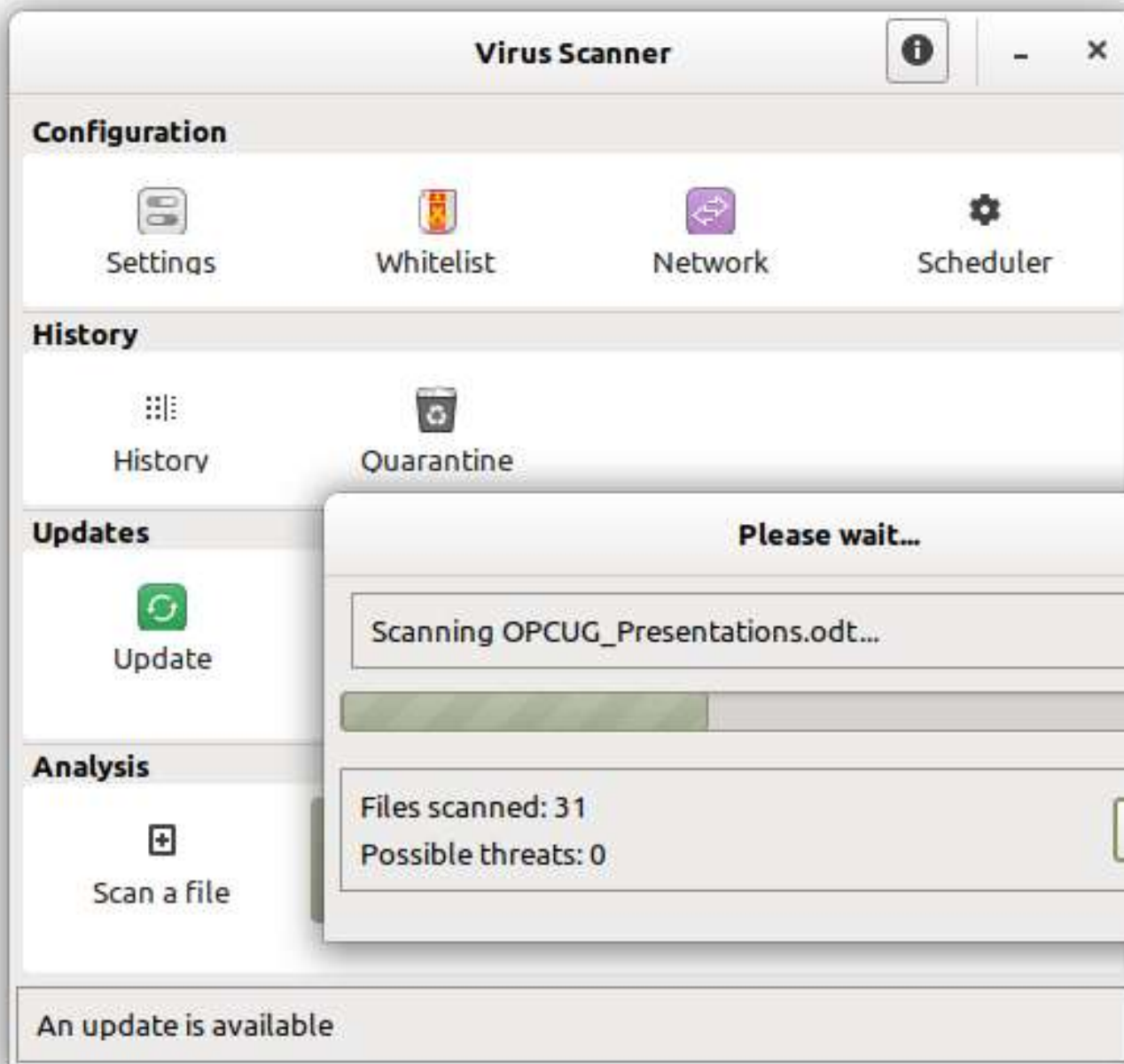


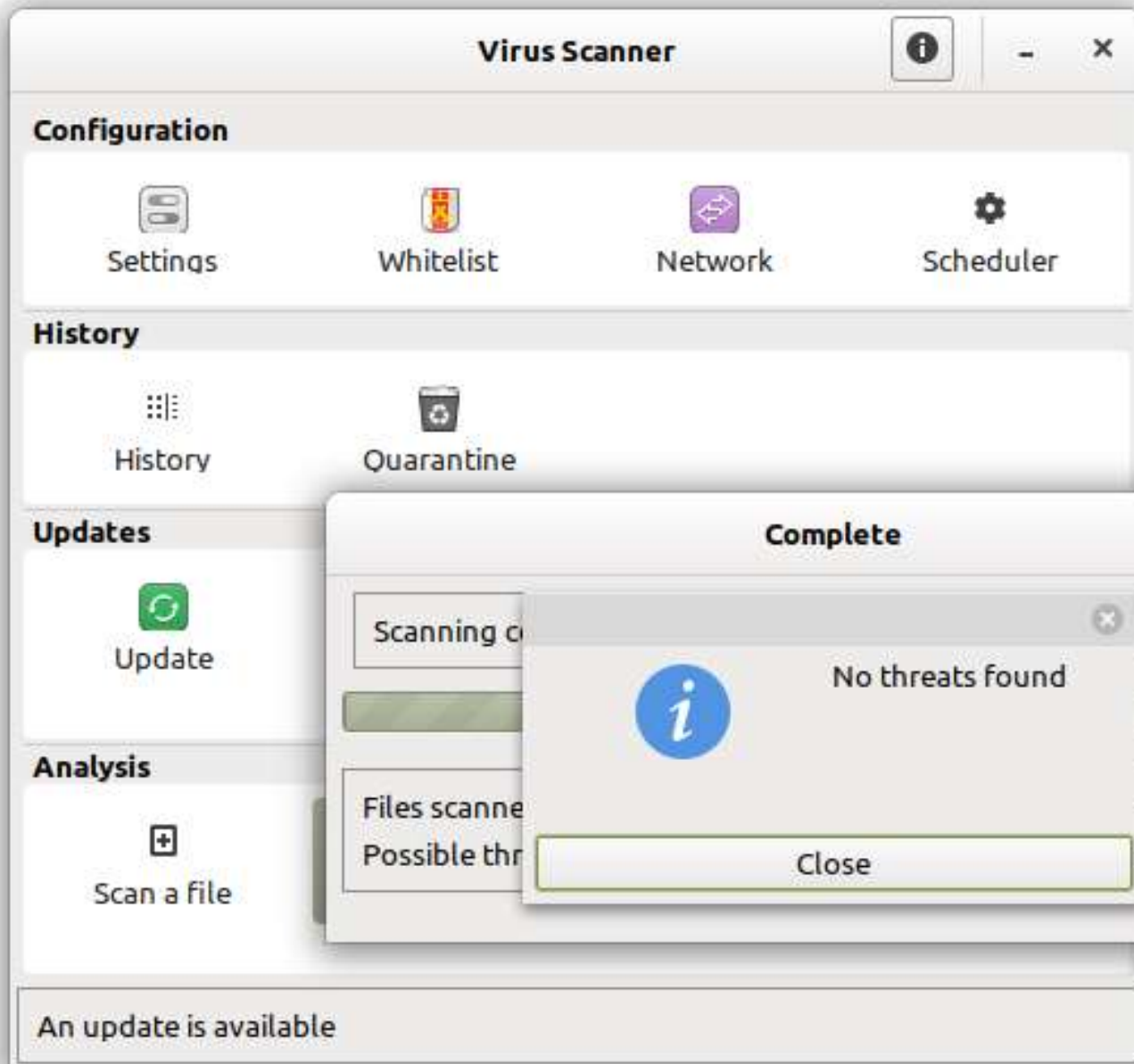












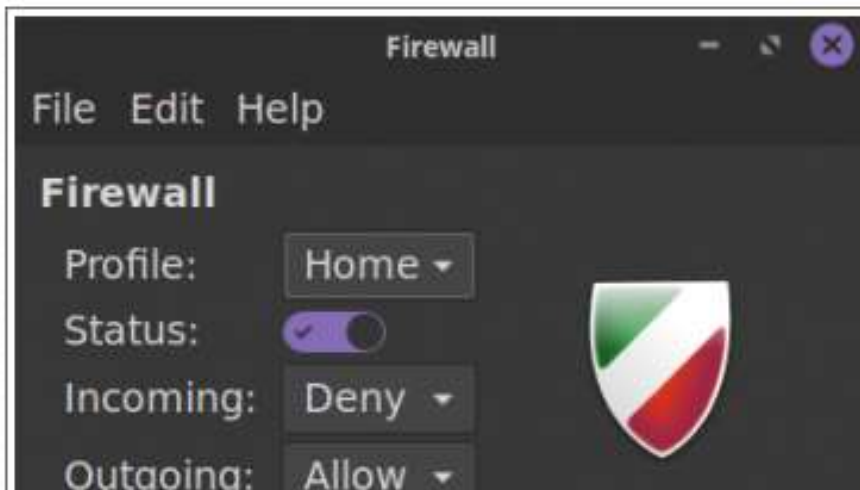
# Linux Mint Firewall

Re: Does LM come w/ a firewall enabled by default?

by spamegg » Mon Jul 13, 2020 5:39 am

It comes with a firewall but it is disabled by default. Go to Menu, type Firewall Configuration, enter your sudo password. Then you can enable it by clicking the Status button:

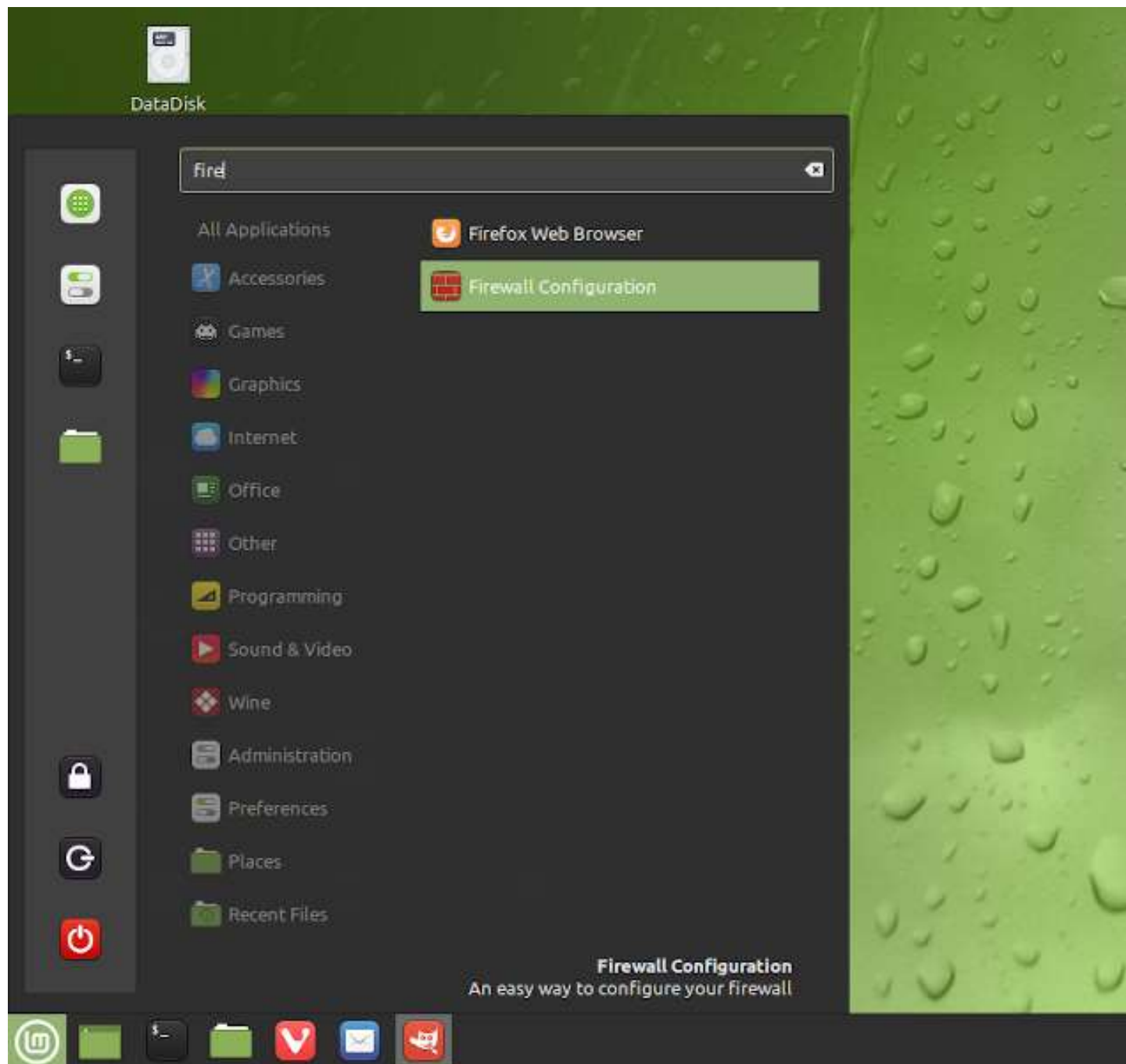
## ATTACHMENTS

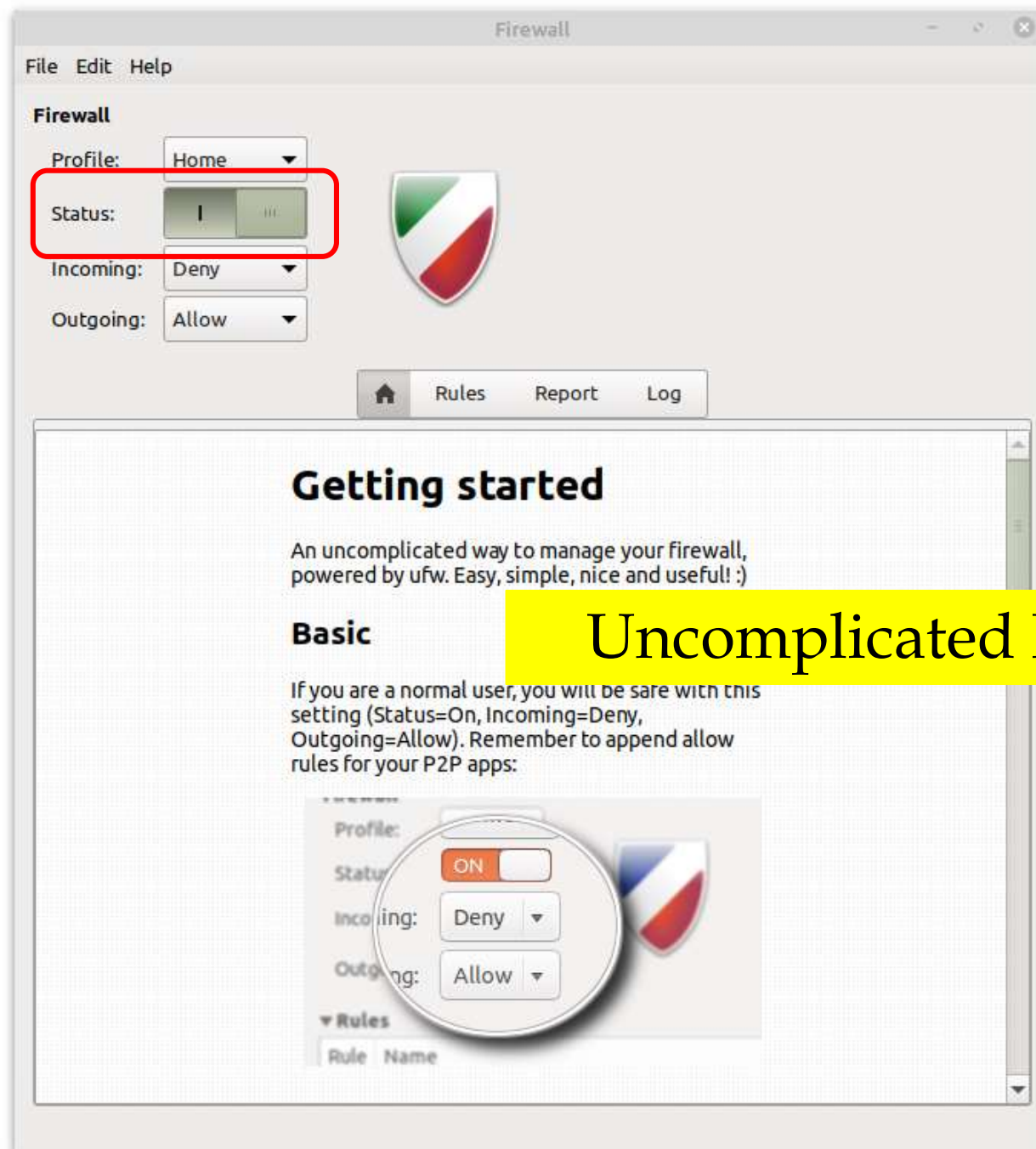


spamegg  
Level 6

Posts: 1420  
Joined: Mon Oct 28, 2019 2:34 am

<https://forums.linuxmint.com/viewtopic.php?t=324747>





# Uncomplicated Firewall

```
toaster@i7-Inspiron: ~  
File Edit View Search Terminal Help  
toaster@i7-Inspiron:~$ sudo ufw enable  
[sudo] password for toaster:  
Firewall is active and enabled on system startup  
toaster@i7-Inspiron:~$
```

sudo ufw enable



OTTAWA

# PC NEWS

Volume 35, Number 8

October 2018

## ARTICLE

### Public DNS Resolvers

by Chris Taylor

**T**he Domain Name System (DNS) was developed because humans can remember a domain name like *opcug.ca* far easier than an IP address like 206.47.13.75. DNS *resolves* domain names to IP addresses.

#### Performance and privacy

Two public DNSs that address performance and privacy are *Cloudflare DNS* and *Google Public DNS*. Both have servers around the world on high-speed connections. Both are free for all. in-

*Quad9* was started in August, 2016. It gets its name from the IP address of the service – 9.9.9.9. It uses over 800 TB of threat intelligence from over a dozen industry-leading security companies to decide what to block. Quad9 doesn't extend blocking to "objectionable" sites such as pornography or gambling.

<https://opcug.ca/Articles/1810NEWS.pdf>

Wireless



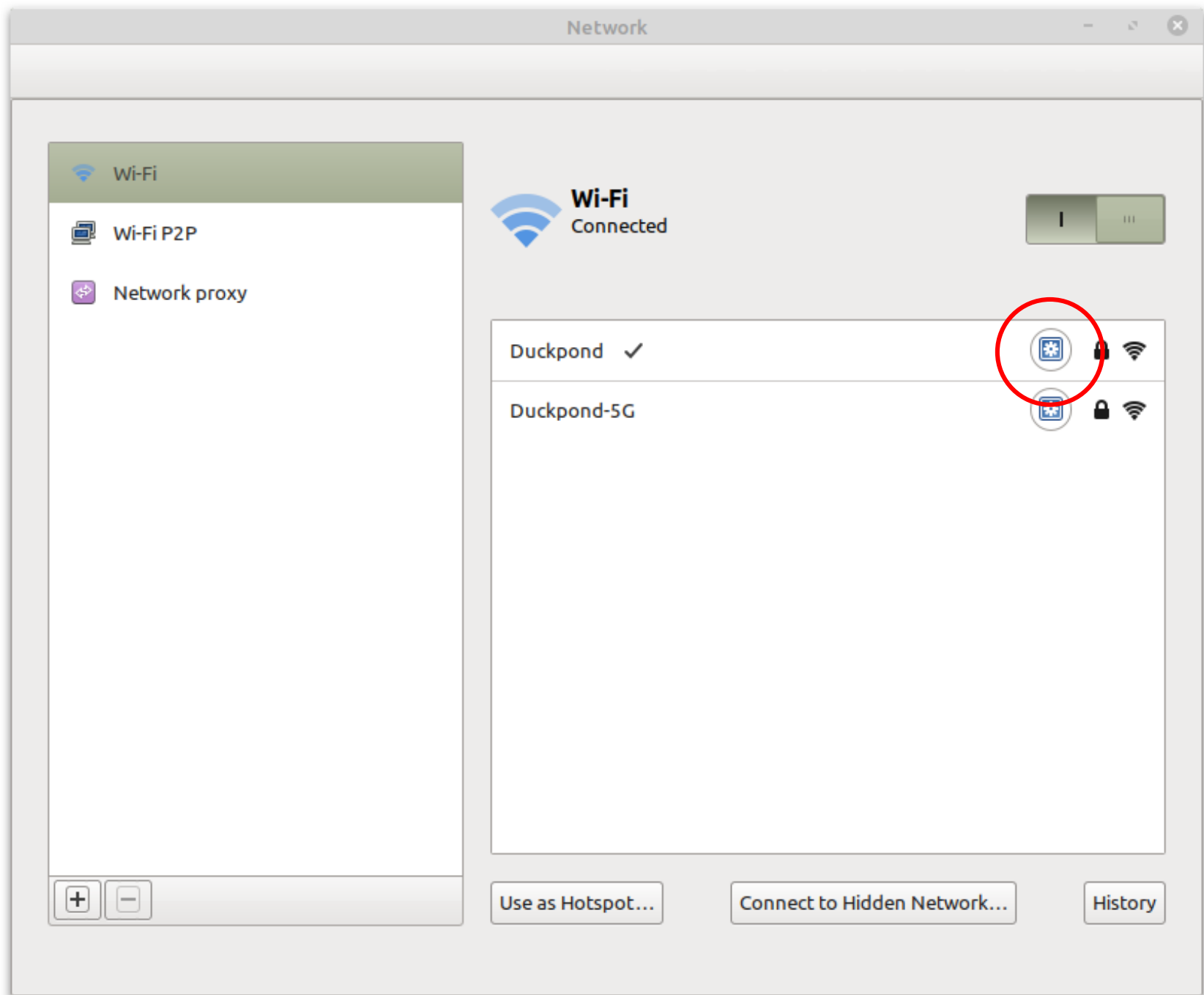
- Duckpond 76% 
- Duckpond-5G 84% 
- NETGEAR31 27% 

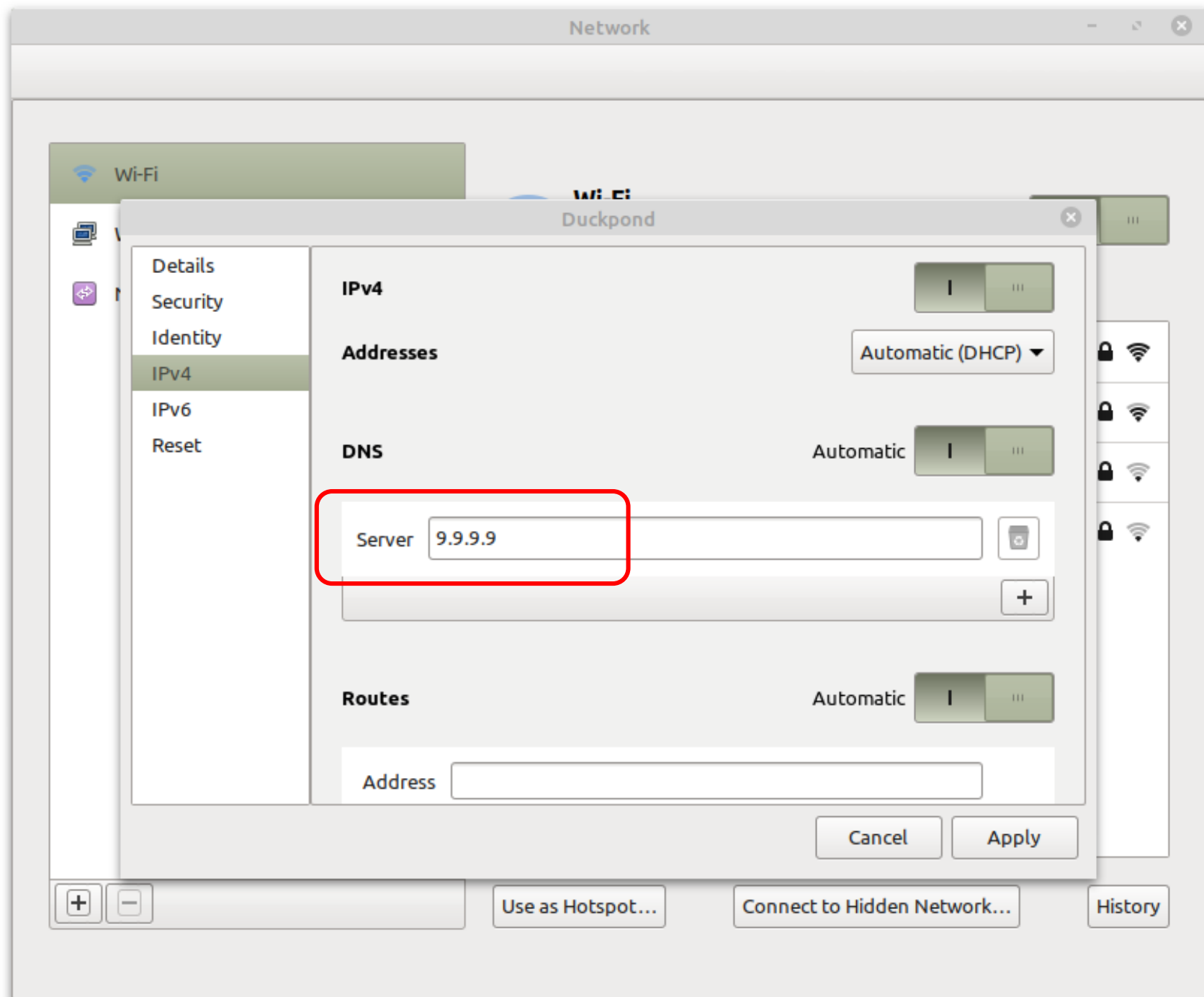
Network Settings

Network Connections



Tue 9 Nov 12:01





# Preparing to abandon<sup>the windows</sup>~~ship~~

To-do list:

- ✓ (1) Install Linux
- ✓ (2) Identify the c
- ✓ (3) Identify Linu
- ✓ (4) Find workarc



Share

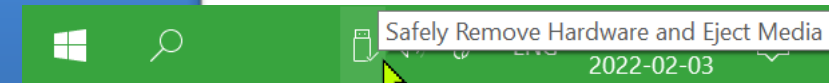
# *Safely Remove* external drives

When you have an external storage device

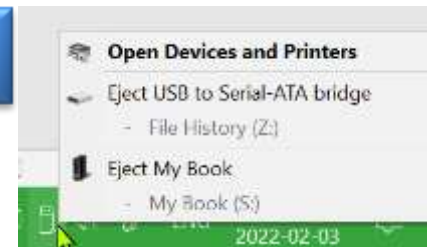
- flash drive, external hard drive, etc.

Windows displays

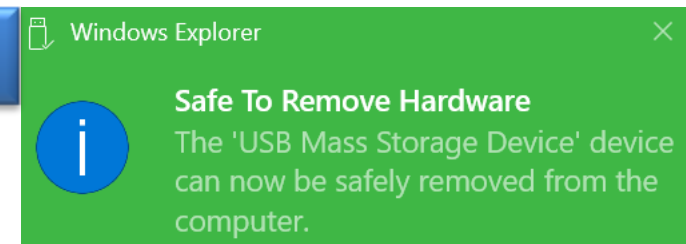
- *Safely Remove Hardware and Eject Media* in system tray (bottom-right section of Taskbar)



Click for listing of external drives



Click on any drive listed to disconnect it



Share

# But do you need to?

In the old days...**definitely**

Information might not have been completely written to drive

- information could be lost/corrupted if you just pulled the drive

Since Windows 10 v1809 (released 2018-11-12)  
Microsoft changed default behaviour for external storage

- **Quick removal:** This policy manages storage operations in a manner that keeps the device ready to remove at any time. You can remove the device without using the Safely Remove Hardware process. However, to do this, Windows cannot cache disk write operations. This may degrade system performance.

<https://docs.microsoft.com/en-US/windows/client-management/change-default-removal-policy-external-storage-media>

Share

# So safe to pull?

- **Quick removal:** This policy manages storage operations in a manner that keeps the device ready to remove at any time. You can remove the device without using the Safely Remove Hardware process. However, to do this, Windows cannot cache disk write operations. This may degrade system performance.

As long as you don't have any open files on the drive

- you can just pull the external drive and not lose anything

You **know** you have no open files, right?  
...that's what I thought  
...me neither

Sometimes when I try to **Safely Remove**

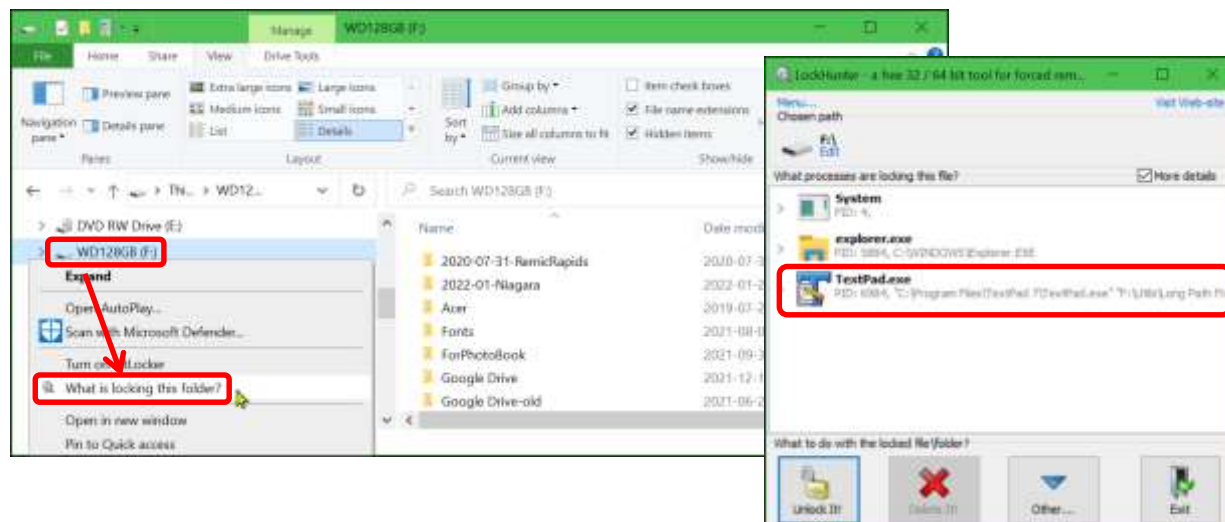
- even when I **know** I don't have any open files on the drive



Share

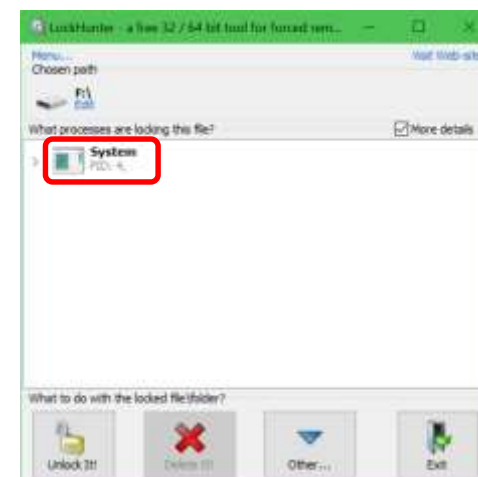
# What program is using device?

- LockHunter
  - can tell you what programs are “locking” the drive
  - right-click any file/folder/drive
    - choose *What is locking this file/folder*



Oops – I **do** have an open file

- data could be lost if drive pulled



System, Explorer

- **shouldn't** be of concern

<https://lockhunter.com/>

Share

## Bottom line

- I still think it is safest to use
  - **Safely Remove Hardware and Eject Media**
- If I get a message



- I use LockHunter to see if I have any files open
- if not, I pull the drive

But I still wonder...

- is it okay to pull if **System** or **Explorer** are “locking” drive?
- absolute safest: do a **Sign out** or **Shut down**
  - please tell me if I am being overly paranoid!

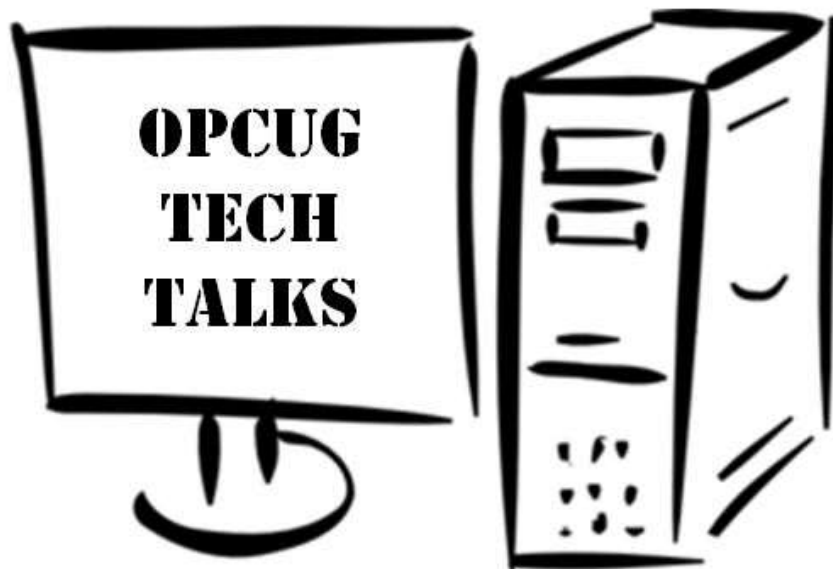
# Privacy Online



## Part 6 – Privacy Policies



**Any other:  
Questions  
Comments  
Shares?**



A monthly series of Tech Talks that will be free to OPCUG members and available to non-members for a registration fee of \$20 - which will include a one-year membership in the club!

See the up-coming March newsletter for details....

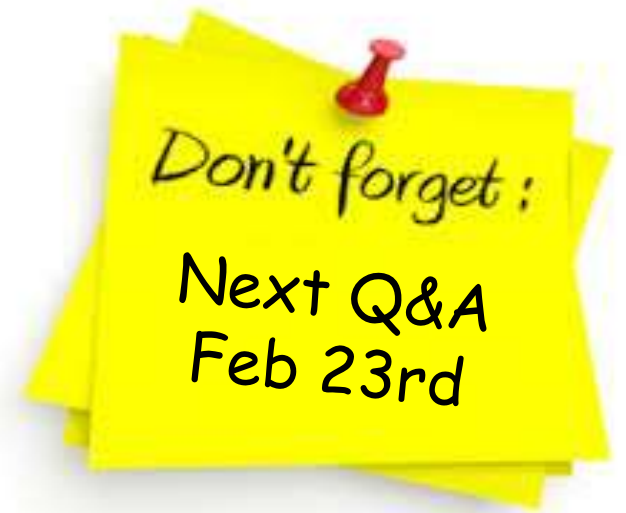
# Two Good to Miss!

- Join OPCUG before March 31<sup>st</sup>
- Pay the annual membership fee of \$20.00
- Receive a free-year's membership

**Two years for  
the price of one!**

<https://opcug.ca/join-or-renew/>





**Send your questions,  
answers, and topics  
you wish to share to:**

**[SuggestionBox@opcug.ca](mailto:SuggestionBox@opcug.ca)**

