

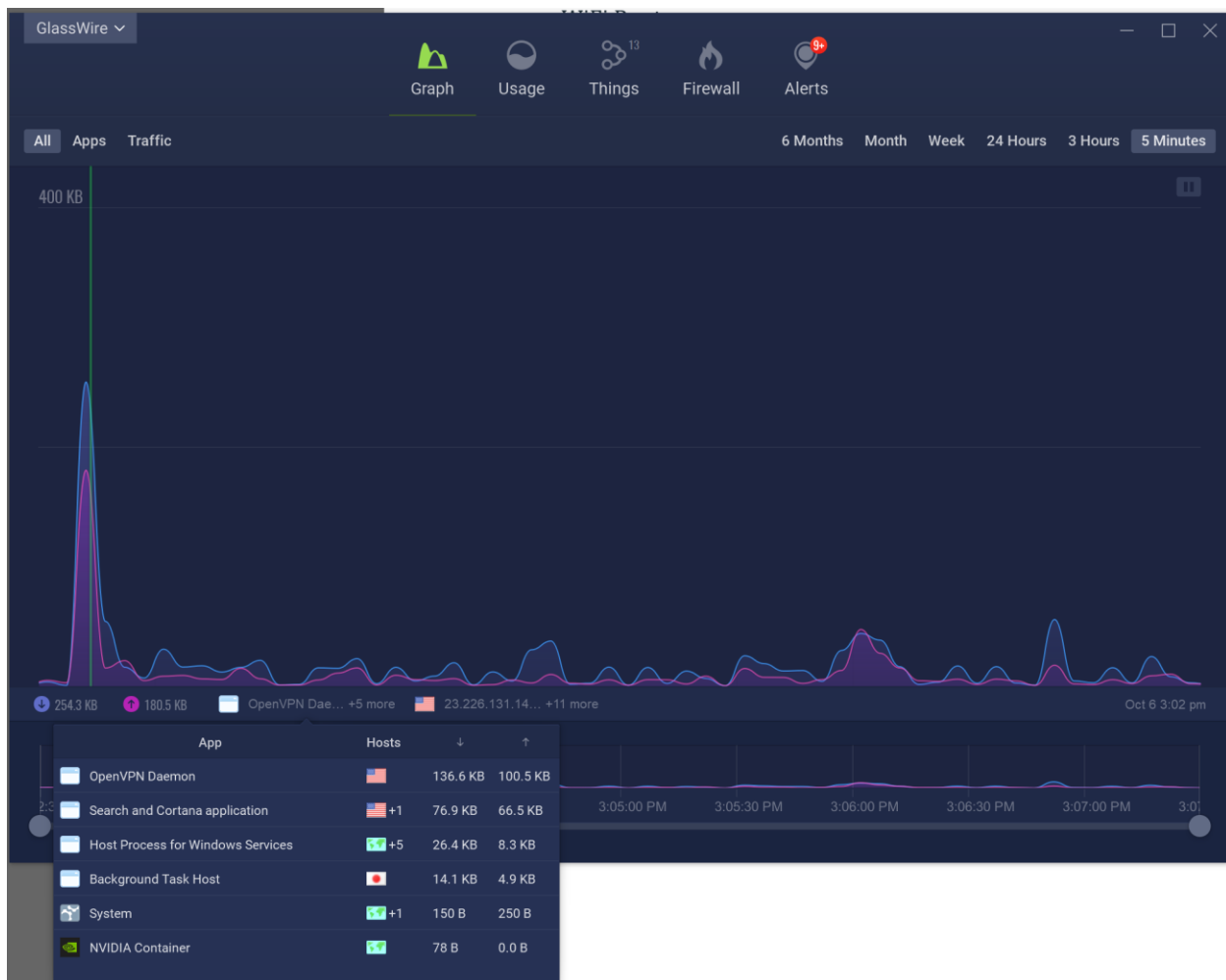
Personal Risk Assessment

In my personal risk assessment, I focus both on configuration and user awareness. There are so many times that I feel uneasy using my PC to handle PII or other sensitive information, so I wanted to make myself feel more confident in this regard. The following steps were taken to protect myself and bring situational awareness to the forefront of my mind.

GlassWire

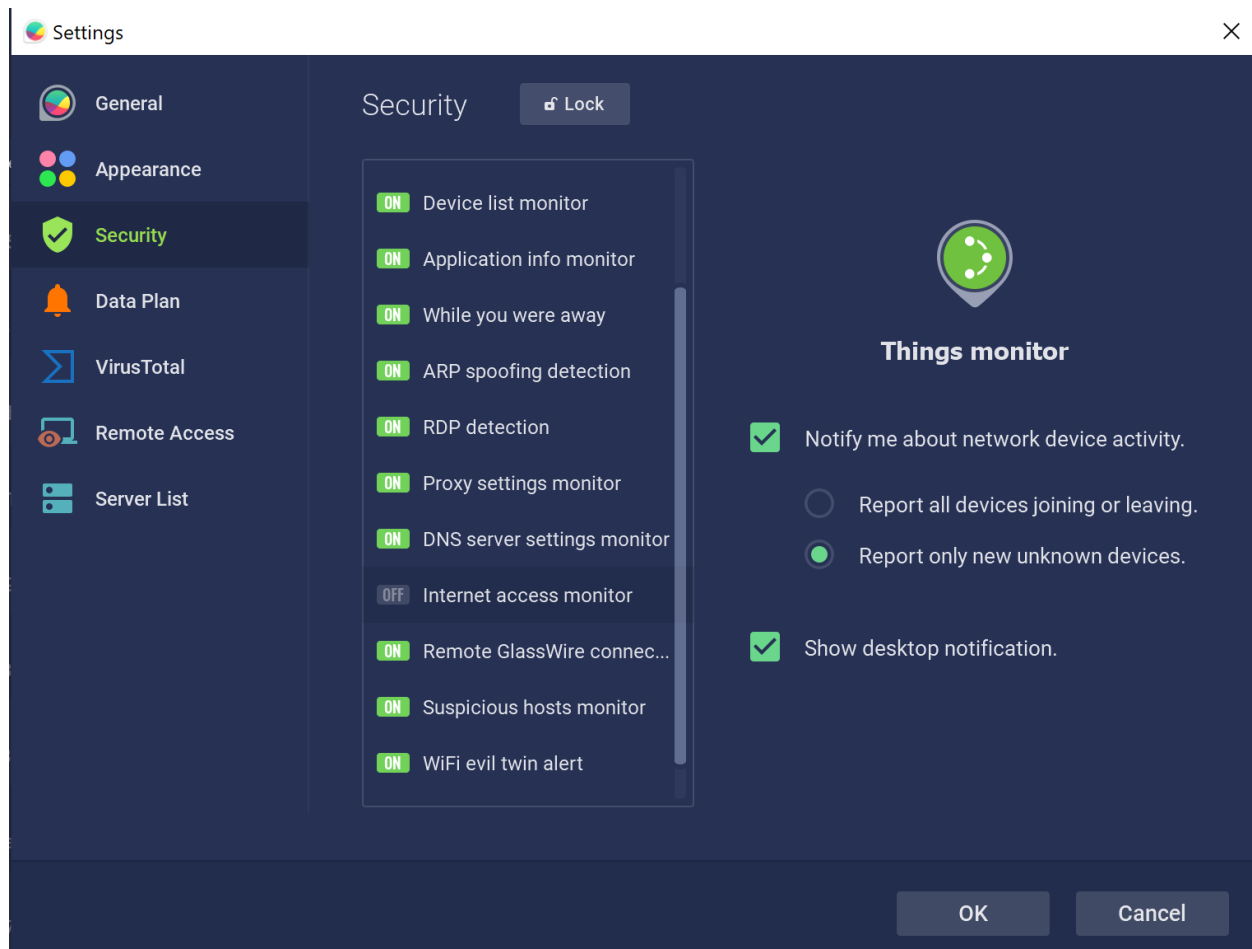
First, I wanted to gain awareness to what my machine is sending and receiving on an attached network. Per my instructor's recommendation, I purchased and installed GlassWire. This application provides valuable information on not just the network traffic, but also the responsible application for sending/receiving the data.

The interface opens up with a timeline graph displaying data sent and data received. This is a cool feature if you just want a quick look at the quantity of flow. Finding the applications responsible is just a click on the graph followed by a breakdown that subsequently appears.



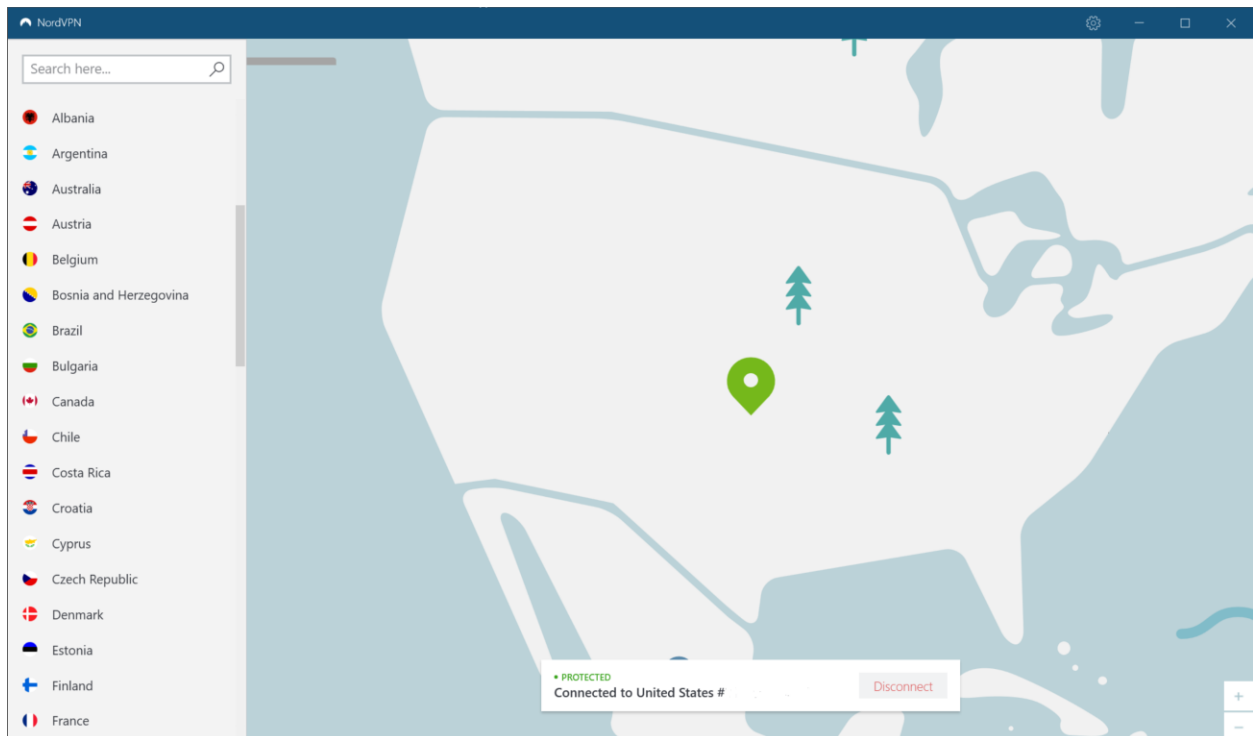
There are useful features in GlassWire that I occasionally use, like reviewing usage history. What I find most useful are the alerts. Once you have gone through the setting to identify what alerts are

important to you, it is really easy to stay aware of network activity based on the notifications that pop up.

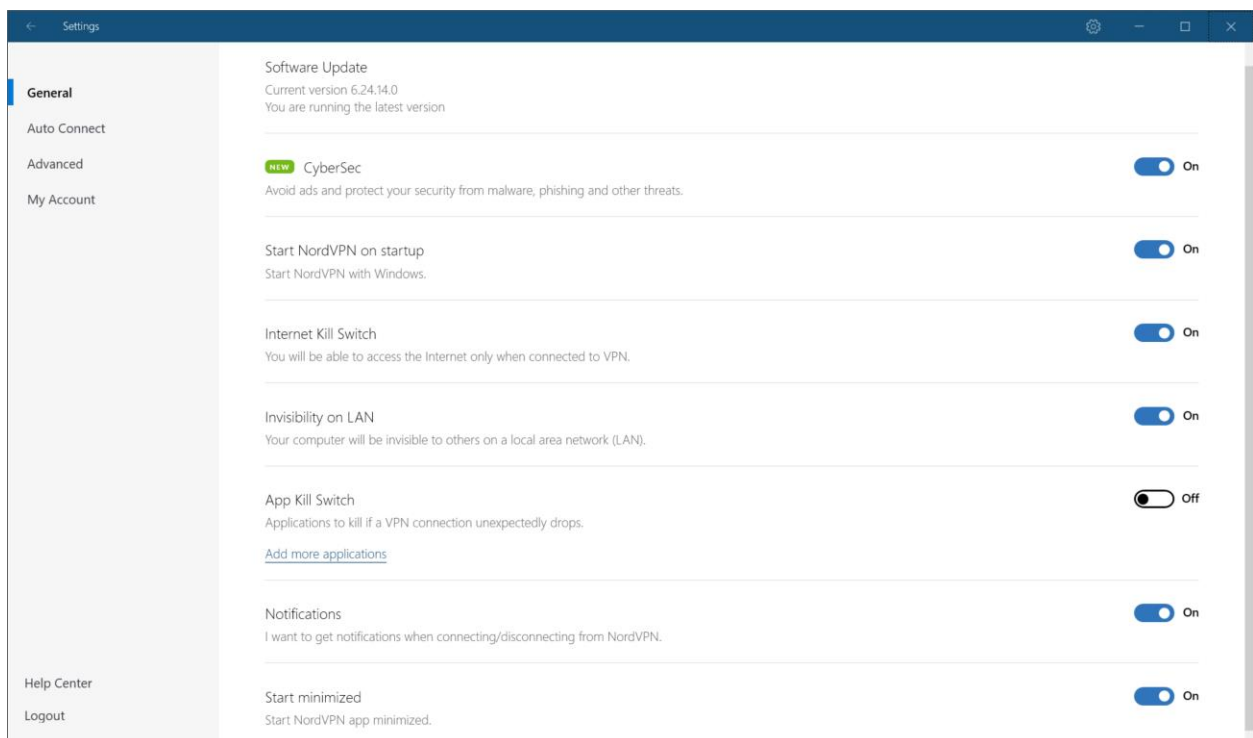


VPN

With my new found awareness of network behavior, I finally went through the effort to purchase and apply a VPN service on my devices. There are so many apps and services that I am only peripherally aware of that send traffic on any available network. I wanted to increase the chances that the traffic will get to its destination without being captured or compromised in some way. After some research, I decided to purchase and install Nord VPN.



After some initial configuration, this is mostly an out of sight out of mind security enhancement. I do change some options depending on my environment. When I am out on shared WIFI, I make sure that I have “Internet Kill Switch” and “Invisibility on LAN” enabled. I have no reason to be identifiable on a shared network and I want to prevent any traffic from being sent through a non-encrypted connection.



EULA Searches

Given what I have learned in this class, I have a slightly sharper view of the EULAs that cross my path. Before clicking the OK button, I spend at least a few moments on the contract. My approach it to do a search for keywords that I think will lead me to information I find important. I generally find some good results around the word “share”.

The screenshot shows the VirusTotal website with a search for the word "share" in the Terms of Service. The search results are displayed on the right side of the page, highlighting several instances of the word "share" in various contexts. The left sidebar contains navigation links such as "Back Home", "How it works", "Terms of Service", "Privacy Policy", and "Join Us". The main content area on the right lists search results for the word "share", including sections like "Safe Participation in the Community" and "Sample & Community Content Guidelines".

Find on page: **share** 6 of 7 Options

VIRUSTOTAL

Search

Back Home

How it works

Terms of Service

Privacy Policy

Join Us

attack, or attempt to attack our Site via a denial-of-service attack or a distributed denial-of service attack;

- use or allow any third party under your control to submit Samples that are subject to the International Traffic in Arms Regulations ("ITAR") maintained by the U.S. Department of State or do any other thing to cause CSIL to provide a defense service as defined by the ITAR, or
- otherwise use the Service except as expressly allowed under these Terms.

Safe Participation in the Community

While VirusTotal has commercial relationships with select members of the Community (organizations, institutions and Partners) public access to the VirusTotal Site is only available free of charge.

VirusTotal offers certain functionality that may require the creation of a personal account (e.g. to participate in the VirusTotal Community). Depending on the information provided in the registration and profile building process, your account may uniquely identify you. Any comment, post or other activity you engage in with the Community when using your account will generate content attributed to you ("Content").

To the extent you use any password/keys/credentials to access the Service, you are exclusively responsible for generating unique and complex credentials, safeguarding them, and for any activities or actions taken on the Service using such credentials.

Sample & Community Content Guidelines

To the extent you elect to contribute any Sample to the Community, you confirm that all content contained in the Sample complies with these Terms and our [Privacy Policy](#), that you are either the original owner of the Sample you submit or that you have the necessary rights and permissions to irrevocably contribute the Sample and **share** it, and information about it, with the Community.

You understand that if you submitting any Sample, the Sample is immediately **shared** for review by the Service's Partners, and the resulting intelligence report is **shared** with you and, with the Partners, which use the results to improve their own systems. As such, by contributing a Sample, you are contributing to the effort to raise global IT security levels.

While you retain any ownership rights in the original material contained in the Sample, when you upload or otherwise submit a copy of the Sample, you give VirusTotal (and those we work with) a worldwide, royalty free, irrevocable and transferable licence to use, edit, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute all content contained in the Sample.

YOU FURTHER AGREE THAT YOU WILL ONLY UPLOAD SAMPLES THAT YOU WISH TO PUBLICLY **SHARE** AND THAT IN ANY CASE, YOU WILL NOT KNOWINGLY SUBMIT ANY SAMPLE TO THE SERVICE THAT CONTAINS CONFIDENTIAL OR COMMERCIAL SENSITIVE DATA OR PERSONAL DATA OF ANY INDIVIDUAL WITHOUT LAWFUL PERMISSION.

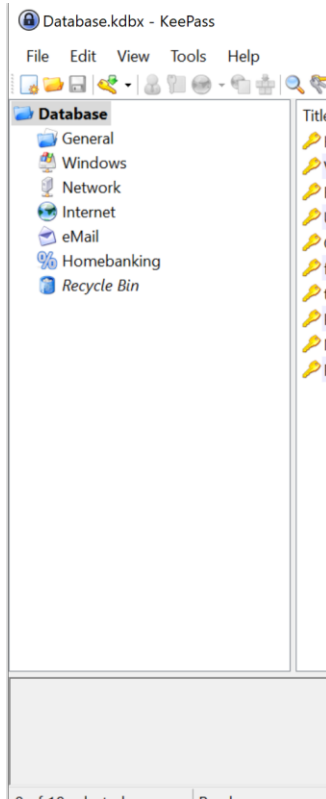
Although we have no obligation to monitor use of the Service, user Content or any Samples, we may monitor the Service to detect and prevent fraudulent activity or violations of these Terms and retain absolute discretion to remove Samples, Content or users from the Service at any time and for any reason without notice. At the same time, to promote the security of the Community and information sharing accountability, accounts and Samples contributed by the Community (for example, comments, posts, etc.) generally will not be removed from the Service, unless they are illegal, violate the lawful rights of an individual, serve any other unethical/malicious purpose, or otherwise violate these Terms.

IF YOU DO NOT WANT TO PUBLICLY **SHARE** A SAMPLE IN THE MANNER SET OUT IN THESE TERMS OR IN THE [PRIVACY POLICY](#), DO NOT SEND IT/CONTRIBUTE IT TO THE SERVICE AS THE SERVICE IS DESIGNED TO WORK THROUGH THE COLLECTIVE AGGREGATION AND SHARING OF THREAT-INTELLIGENCE WITH AND THROUGH THE COMMUNITY.


<http://www.virustotal.com/>


KeePass

Creating a protected database for my passwords greatly saved me time and allowed me to deploy more complex passwords. Offloading that from my mind also had the effect of being correct more often.



In addition to storing the passwords, KeePass has been very helpful in creating passwords matching the specific criteria required by the account policy. I used to spend way too much time on choosing the right password that could be memorized. Now I can just generate a password the exceeds the limited complexity my brain can handle and store it in a secured location.



 Password Generator ✕



Password Generation Options

Here you can define properties of generated passwords.

Settings **Advanced** Preview

Profile: (Derive from previous password)  

Current settings

☒ **Generate using character set:**

Length of generated password:

☒ Upper-case (A, B, C, ...)

☐ Space ()

☒ Lower-case (a, b, c, ...)

☐ Special (!, \$, %, &, ...)

☒ Digits (0, 1, 2, ...)

☐ Brackets ([,], {, }, (,), <, >)

☐ Minus (-)

☐ High ANSI characters


☐ Underline (_)

Also include the following characters:

☐ **Generate using pattern:**

☐ Randomly permute characters of password

☐ **Generate using custom algorithm:**



☐ Collect additional entropy

Help

OK

Cancel

OSINT

The resources provided by OSINT have been very useful in aggregating available data, or just for quick lookups. I learned a lot about the information available on myself, as well as information that can be gathered from information associated with me, like my phone number or license plate.

