**Lab 3:** The installation, Configuration, and Testing of Tools Snort and Veracrypt

**Security Team:** Luis Ruiz, Marcos Vallejos, Ryan Rockett, Kari Hattabaugh

Table of Contents

[Introduction (Kari) 2](#_Toc86615437)

[Scope (Kari) 2](#_Toc86615438)

[Snort 4](#_Toc86615439)

[Information About Tool (Ryan) 4](#_Toc86615440)

[Prerequisites (Ryan) 4](#_Toc86615441)

[Instructions (Luis) 6](#_Toc86615442)

[Testing 15](#_Toc86615443)

[Recommendations (Kari) 17](#_Toc86615444)

[Alternatives (Marcos) 18](#_Toc86615445)

[Veracrypt 18](#_Toc86615446)

[Information About Tool (Ryan) 18](#_Toc86615447)

[Prerequisites 19](#_Toc86615448)

[Installation (Luis) 20](#_Toc86615449)

[Testing 31](#_Toc86615450)

[Recommendations (Kari) 35](#_Toc86615451)

[Alternatives (Marcos) 36](#_Toc86615452)

[Conclusion (Kari) 37](#_Toc86615453)

[References 38](#_Toc86615454)

# Introduction (Kari)

Ashburn’s Frog Emporium has tasked our security team with developing and implementing an integrated defense in depth strategy regarding their information security. With this we plan to implement two separate tools to satisfy two components of an integrated defense in depth. The first tool we will install is Snort, which is a powerful intrusion detection tool. Snort is designed to detect traffic within the network that is abnormal and trigger an alarm allowing for action to be taken. The second tool is Veracrypt, which allows a user to deposit sensitive documents into a container and password encrypt them. Veracrypt will allow for the obfuscation of sensitive data that is stored on Ashburn’s Frog Emporium’s devices.

# Scope (Kari)

Ashburn’s Frog Emporium is a small scale business, which offers online and in person sales. With the growing need for Information Security and their expanding customer base, Ashburn’s Frog Emporium is looking to improve their security. Through the next 90 days, our team will identify, install, and configure a variety of tools to provide a cost effective layered defense to Ashburn’s Frog Emporium. The network consists of workstations, point of sale devices, and servers. The operating systems used are Windows 10 and Windows Server 2016.

Previously we have installed Wireshark, which captures network traffic and allows an in depth examination of the packet headers. This provides us with insight into the TCP flag, IP addresses, protocols, and ports used. This information can show indicators of an attack. Next, we installed Prometheus, which is used to monitor network traffic and allows for configuration for alarm triggering parameters to be set. This offers network monitoring capabilities to Ashburn’s Frog Emporium’s network. During this lab, our security team focused on data security and the limiting and monitoring of movement within our network. To further monitor movement within the network, we implemented Snort. This tool allows us to configure the alarm system to limit the false positives and negatives based on traditional network traffic for Ashburn’s Frog Emporium.As an alternative tool to snort, we identified Suricata, which is a powerful intrusion detection and prevention system. Once Ashburn’s frog emporium has expanded with a larger network, Suricata would provide a more suitable service without compromising the network's performance. To assist in data obfuscation and limiting the movement within the network we implemented the tool Veracrypt. Veracrypt allows the user to create secure password encrypted containers on a network. This provides data obfuscation for the secure customer data that Ashburn’s Frog Emporium needs to handle and store. As an alternative tool, we have identified Cryptomator, which is a cloud based solution for securely sending and storing data with password protected encryption. If Ashburn’s Frog Emporium were to expand to multiple locations, it would offer protected mobility to their secure data.

This lab outlines the information about Snort and Veracrypt, the prerequisites for each tool, and the instructions for installation configuration and testing.

|  |  |  |
| --- | --- | --- |
| **Layer** | **Description** | **Tools Applied** |
| Physical Security | Measures taken to protect a computer or other network device from theft, fire, or environmental disaster. |  |
| Authentication and Password Security | Password policies, identity verification, etc. |  |
| Operating System Security | Maintaining and managing OS patches |  |
| Antivirus Protection | Protection the network and connected devices from malware. |  |
| Packet Filtering | Blocking or allowing the transmission of packets based on configured criteria. |  |
| Firewalls | The tools installed and configured to manage traffic on a network, including firewall policies. |  |
| Demilitarized Zone (DMZ) | The area on the exterior of the network, which focuses on accessibility and the network’s perimeter security. |  |
| Intrusion Detection and Prevention Systems (IDPS) | Technology used to detect and, in some cases, produce an automated response to signatures, or patterns on suspicious network activity. | Prometheus, Snort |
| Virtual Private Network (VPN) | Technology that allows for secure communication using public internet connection. |  |
| Network Auditing and Log Files | Recording and organizing network activity and performance to allow for analytics. | Wireshark, Prometheus |
| Routing and Access Control Methods | Tools that control or limit movement into and throughout the network. | Veracrypt |

# Snort

## Information About Tool (Ryan)

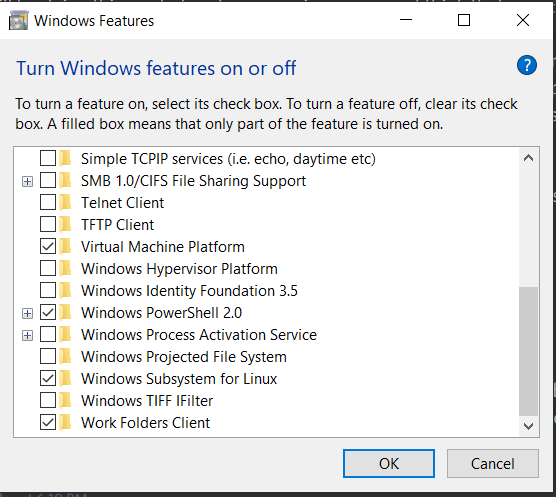
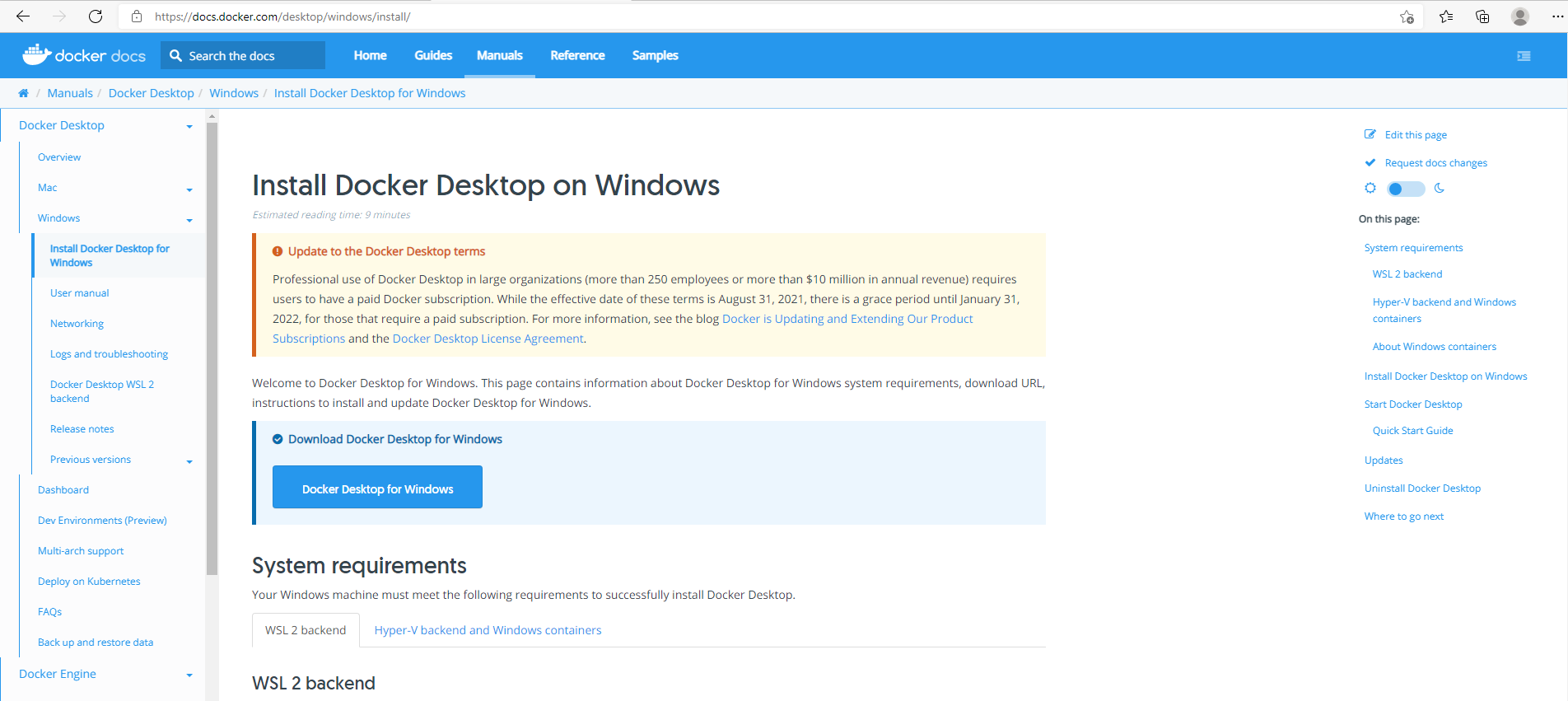
Snort is a free, open source traffic analysis tool that is designed to capture and monitor network traffic in real time. Snort allows you to monitor real time traffic through your network and detect threat events such as an attack.

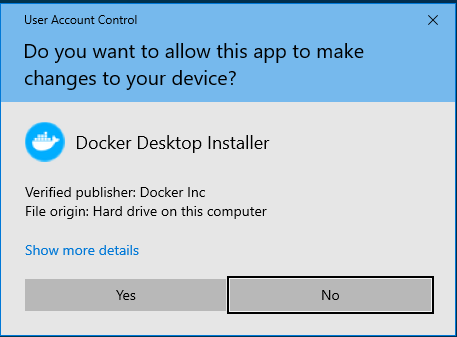
While Snort is free for anyone to download, there are more up to date rule sets that users are able to get, however these are often done by subscription. Users do not need a subscription however to create their own rule sets or use the free community rule sets found on the main Snort website to monitor their network with. Snort is a network-based IDS/IPS, meaning that it is not confined to a single host but instead is used to monitor entire networks. The rule sets define what Snort monitors for on the network. After establishing rulesets, users are able to monitor for activity that would break those predefined rules. Once those rules are broken, the user is able to track and find the source of the issue. Snort rules are different from using signatures because what the user is monitoring is actually the vulnerability itself and the user is looking for an exploit.

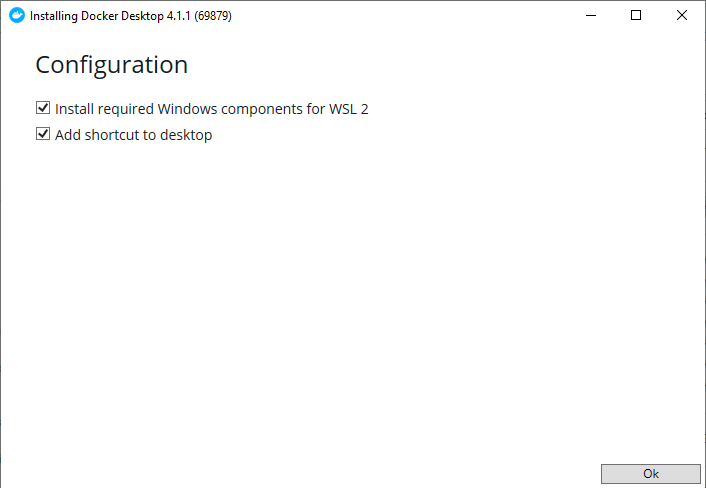
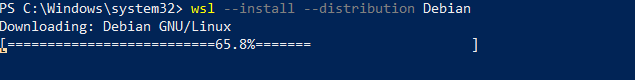
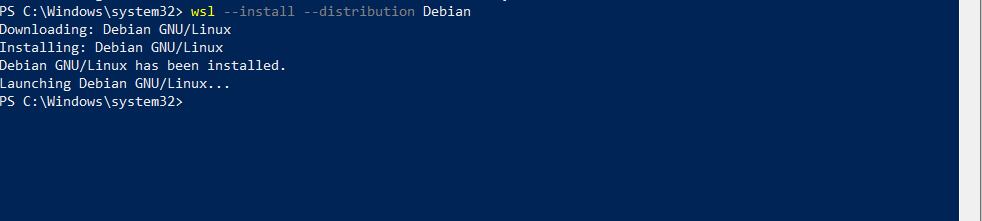
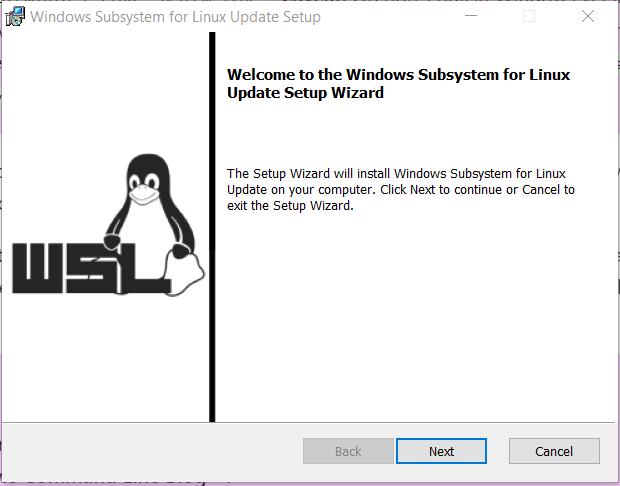
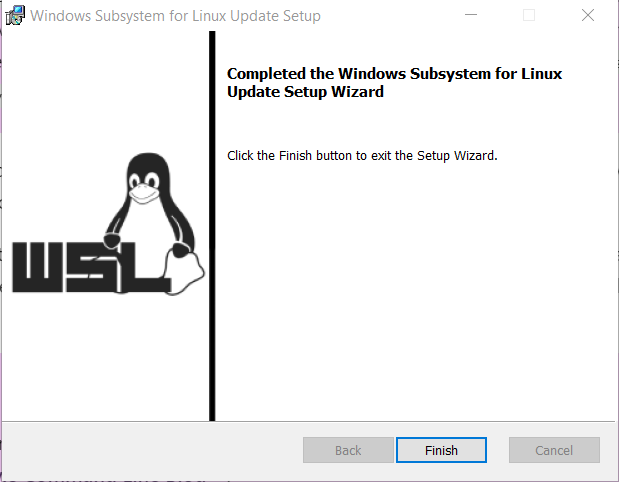
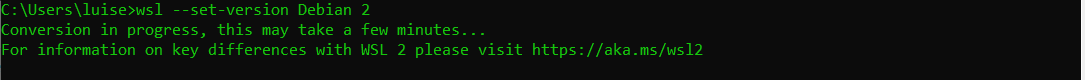
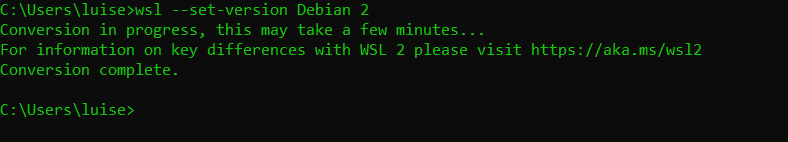
## Prerequisites (Ryan)

* If you are going to download and install Snort for a Windows machine, the user will need to have the downloaded and installed Docker. In addition to Docker, the user will need to select a distribution of Linux to run with Snort, such as Debian.
* Docker has the following system requirements:
  + WSL 2 backend
    - Windows 10 64-bit: Home or Pro 2004 (build 19041) or higher, or Enterprise or Education 1909 (build 18363) or higher.
    - Windows 11 64-bit: Home or Pro version 21H2 or higher, or Enterprise or Education version 21H2 or higher.
    - Enable the WSL 2 feature on Windows
* In order to run WSL 2 on a Windows 10 or Windows 11 system you must have a 64 bit processor with Second Level Address Translation, 4 GB of memory, and BIOS level hardware virtualization.
* If you are going to download and install Snort3 for a Windows machine, you must have the most recent binary and support files in addition to making sure that WinPcap is installed on the machine.
* Snort3 is not officially supported by an operating system. It can work on all nix machines. The following operating systems are known for running Snort without issue:
  + Alpine 3.10/i386
  + Alpine 3.10/x86-64
  + Centos-6-9/i386
  + Centos-6-9/x86-64
  + Centos-7-4/i386
  + Centos-7-4/x86-64
  + Debian-8/i386
  + Debian-8/x86-64
  + Debian-9/i386
  + Debian-9/x86-64
  + Fedora Core 27/x86-64
  + Fedora Core 30/x86-64
  + FreeBSD-11-1/i386
  + FreeBSD-11-1/x86-64
  + FreeBSD-12-0/x86-64
  + OpenBSD-6-2/i386
  + OpenBSD-6-2/x86-64
  + OpenBSD-6-4/i386
  + OpenSUSE LEAP 15.0/x86-64
  + OpenSUSE LEAP 15.1/x86-64
  + OpenSUSE LEAP 42.3/x86-64
  + RHEL-6-0/i386
  + RHEL-6-0/x86-64
  + RHEL-7-0/x86-64
  + RHEL-8-0/x86-64
  + Ubuntu 17.10.1/i386
  + Ubuntu 17.10.1/x86-64
  + Ubuntu 18.04 LTS x86-64
  + Slackware-14.2/x86-64
  + Windows 7 or higher
* At least 7.6 MB of local disk storage.
* While there is no memory requirement, it is recommended to not have a low amount of RAM as that is what is used to perform traffic analysis.

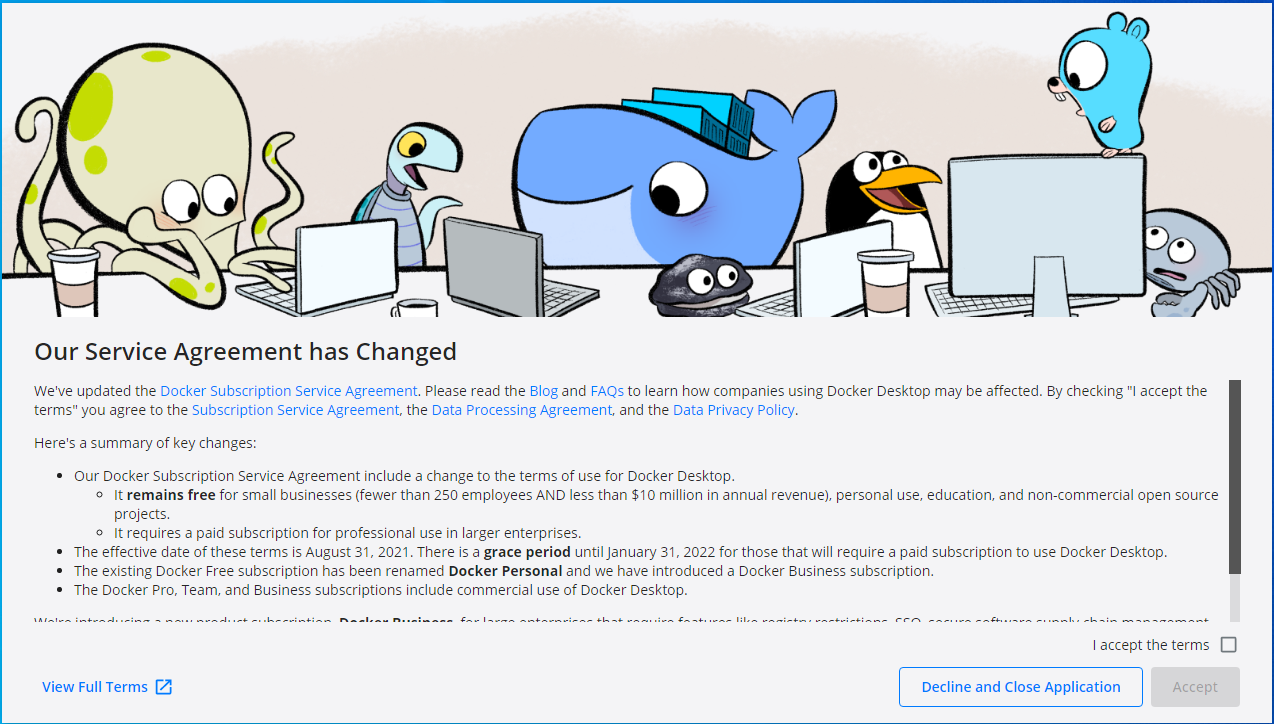
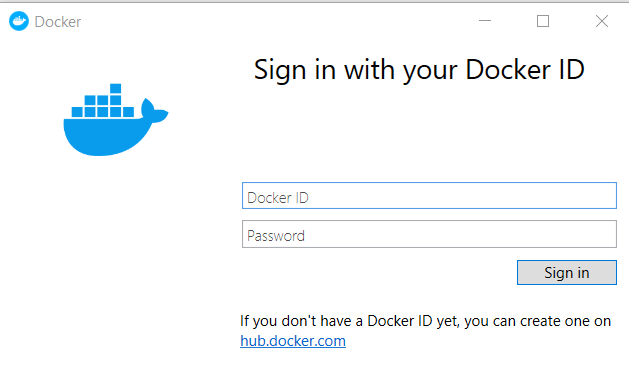
## Instructions (Luis)

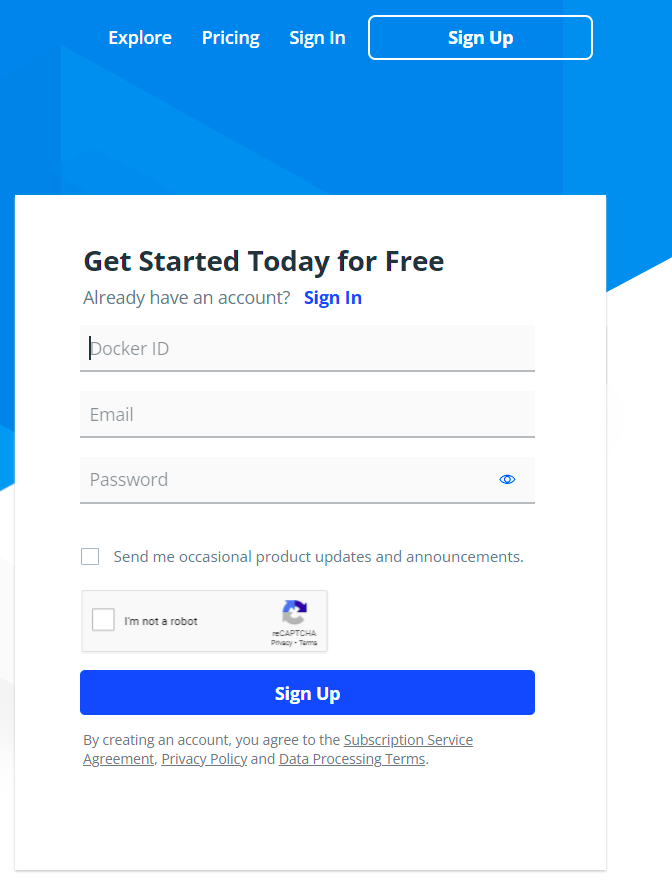
1. The first step that we will be taking will be to go to “Turn Windows features on or off”, this can be accessed by typing that name in the windows search bar and clicking the result or through the control panel. Once we are in the Windows Features screen, we will scroll down and select “Virtual Machine Platform” and click to select “Windows Subsystem for Linux” if they were not already enabled. Our system came with both these features enabled, if yours was not you will be prompted to restart the system. Restart your system to continue. This is a vital step and if these are not selected, then we will not be able to proceed with the docker installation or Snort3 installation. ****
2. Now we will go <https://docs.docker.com/desktop/windows/install> Read all the system requirements. The instructions will also go over on how to meet the requirements if you are not compliant with them. Click on Docker Desktop for Windows to begin the download. 
3. Click on the Docker Desktop Installer
4. Click Allow

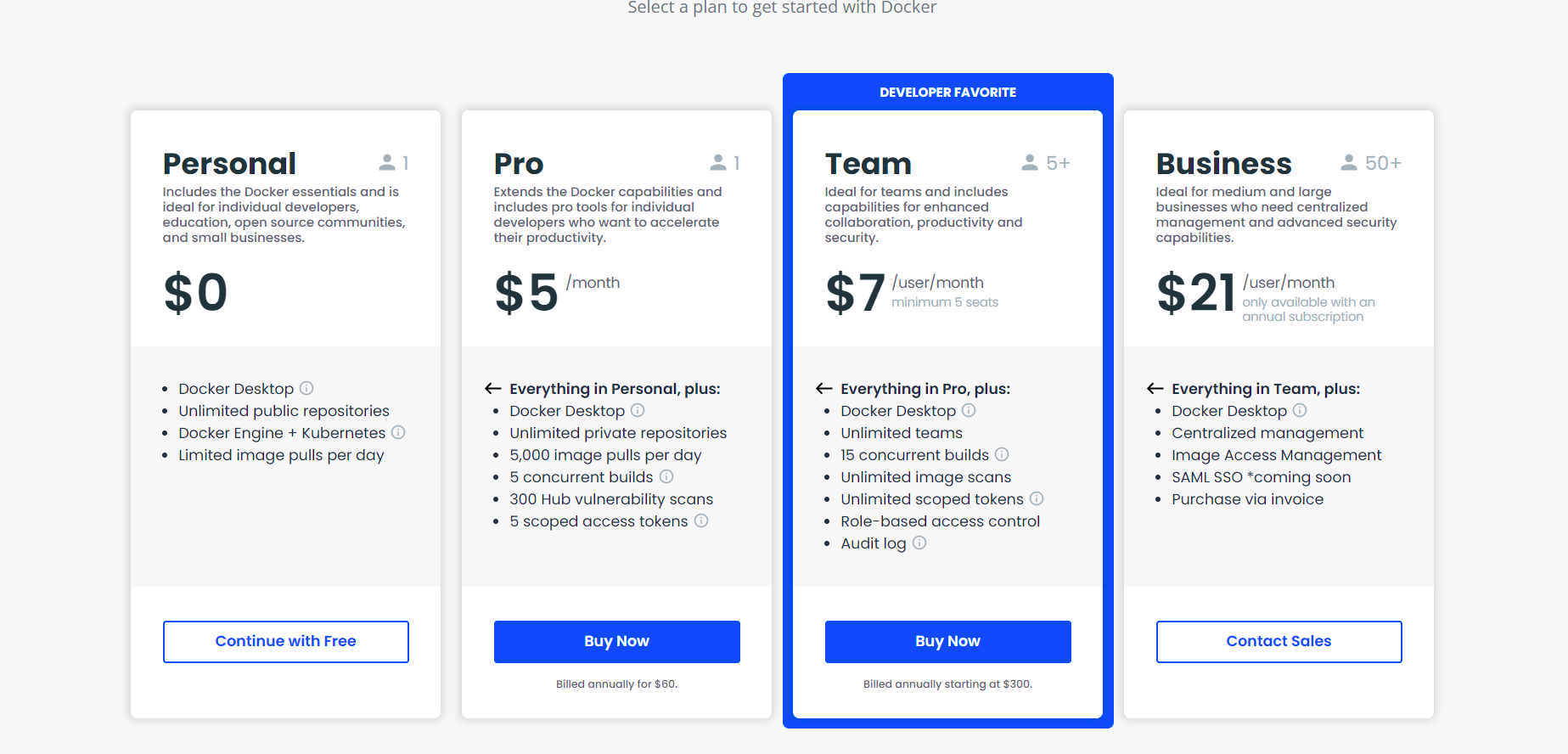
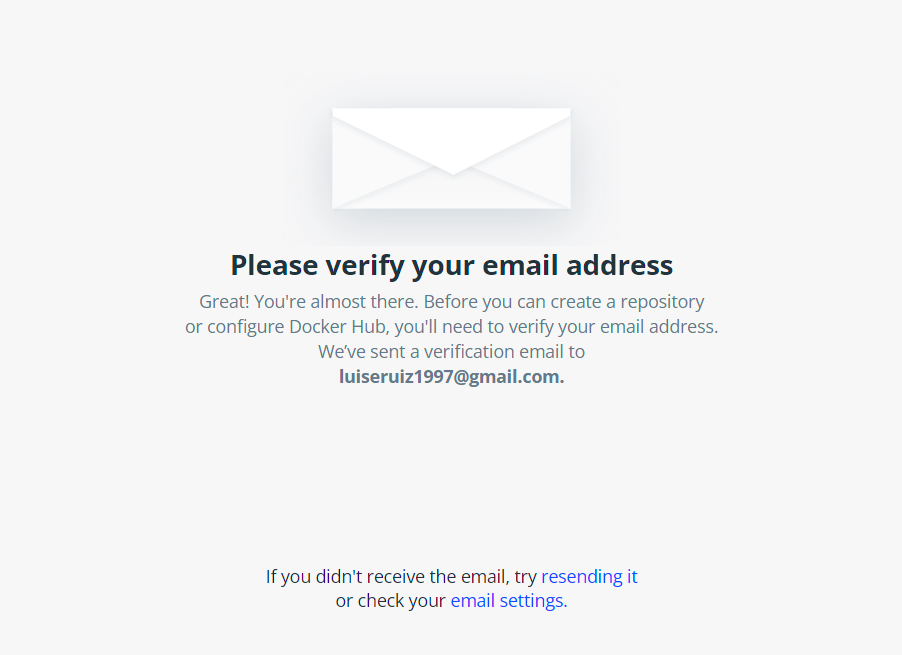
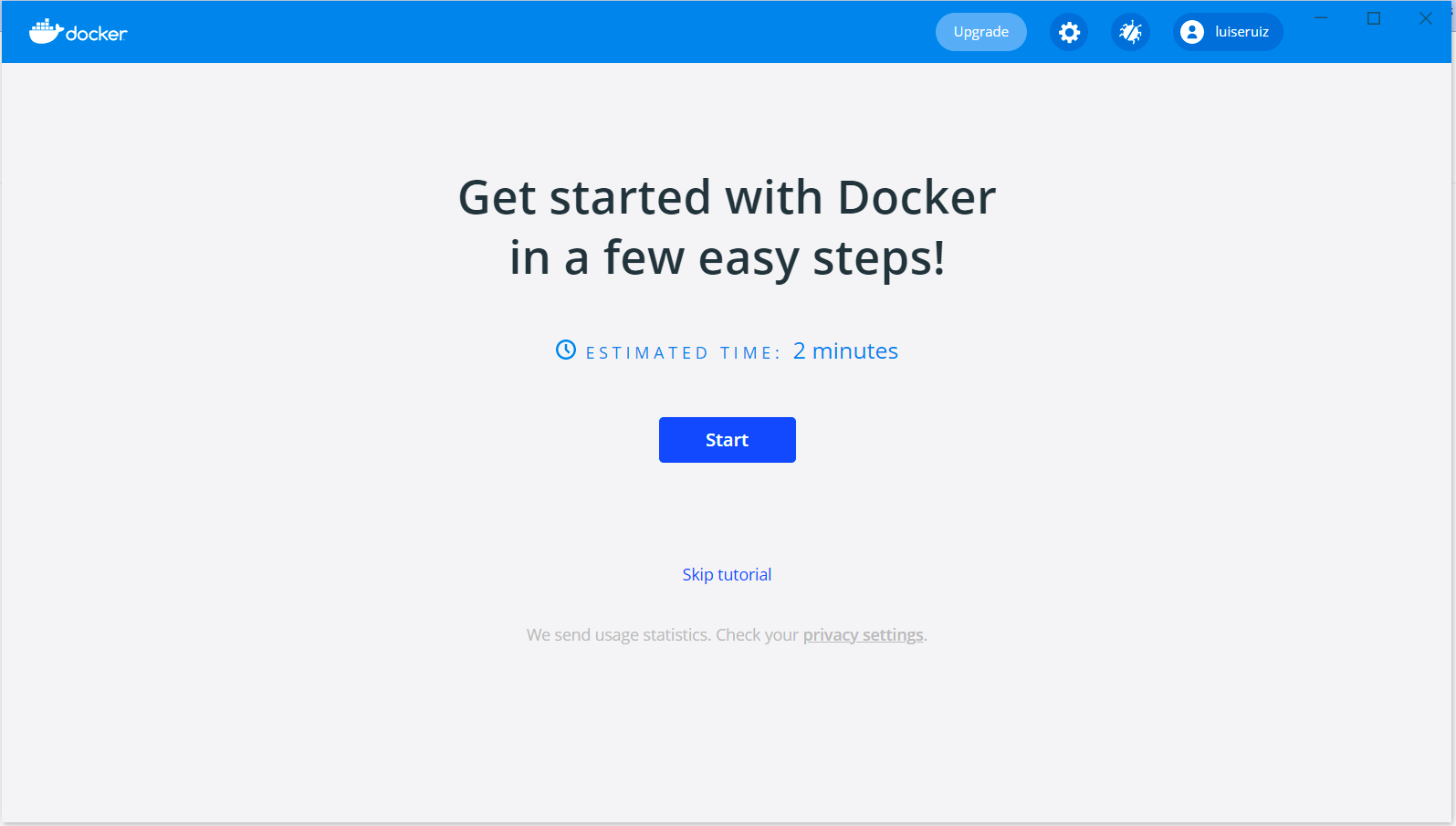
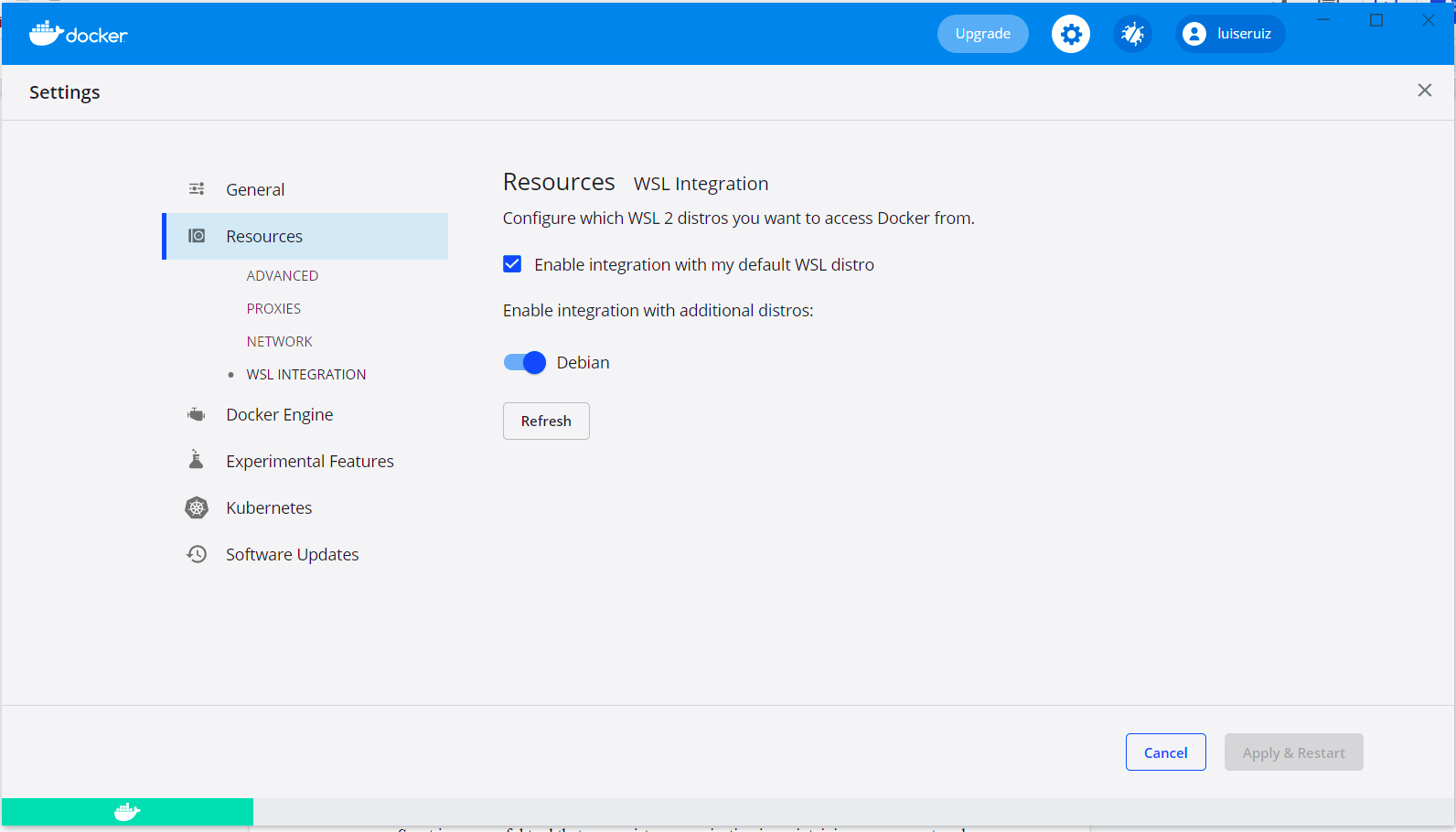
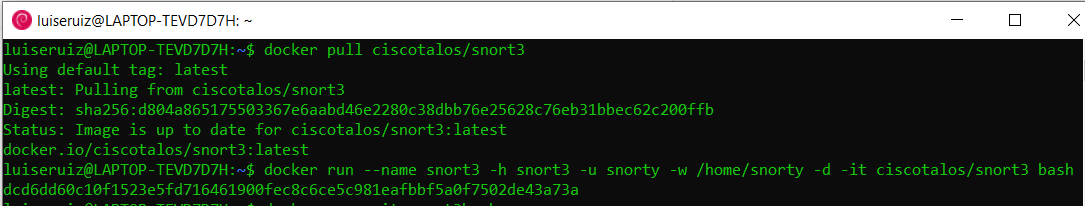


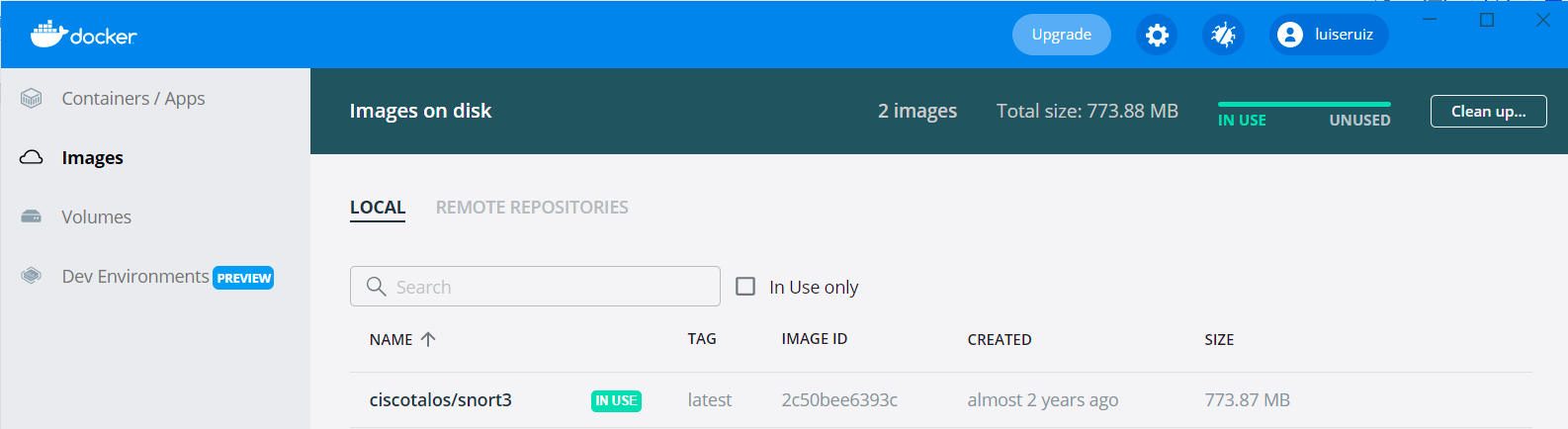
1. Make sure both options are checked then click okay. Docker will begin to install once the installation is complete, restart your computer. Do not open Docker yet or you will see errors. We will now proceed to install a Windows Subsystem for Linux and Debian. 
2. If you recall to Step 1, we have allowed for WSL and VMP features on our windows device. Now we will run windows PowerShell as the administrator and type in “wsl --install --distribution Debian” This will install the Linux distribution that we will use with Snort3. 
3. Wait until it is installed and launches. You can close out of it; it is not necessary to keep open yet. 
4. Next, we will update the WSL, this is necessary to ensure stability with dockers. 
5. Click Finish
6. Now go to “<https://docs.microsoft.com/en-us/windows/wsl/install-manual#step-4---download-the-linux-kernel-update-package>” and click on “WSL2 Linux kernel update package for x64 machines” 
7. Now we will convert Debian to WSL2 from its default WSL1. open your command line interface and type “--set-version Debian 2” check for correct capitalization and click enter. 
8. Wait until the conversion is complete. 
9. Now we will open up docker. It will be on your desktop or you can search for it in the windows search options.



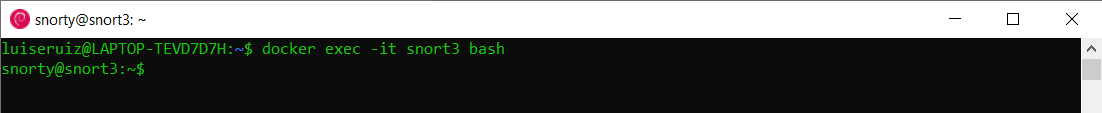
1. Read the Service Agreement, since we have fewer than 250 employees and make less than $10 million in annual revenue we can use the free version. 
2. Next we will need to sign in to Dockers, since we do not have an account we will need to register an account. 
3. Create a Docker ID, enter your Email, create a password then sign up. You will later receive a confirmation email.

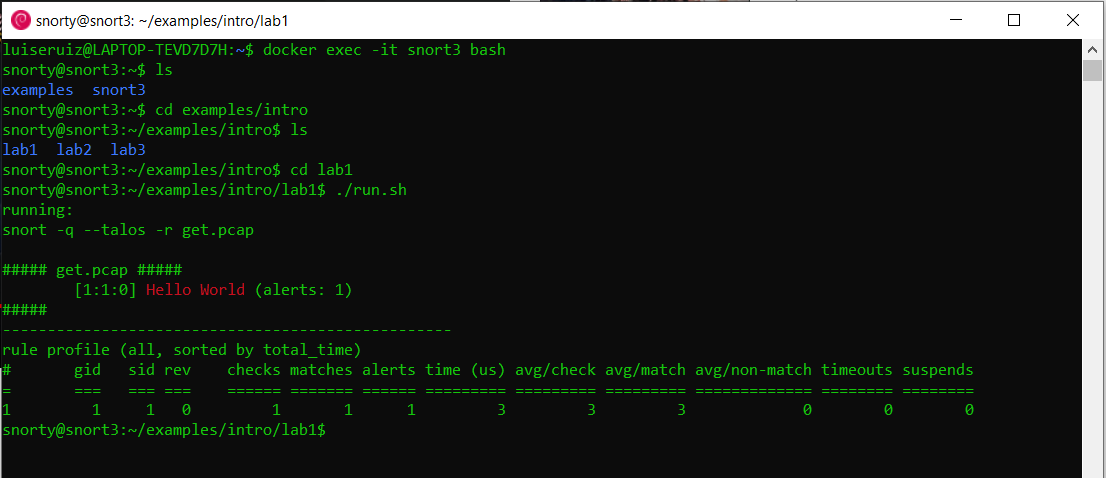
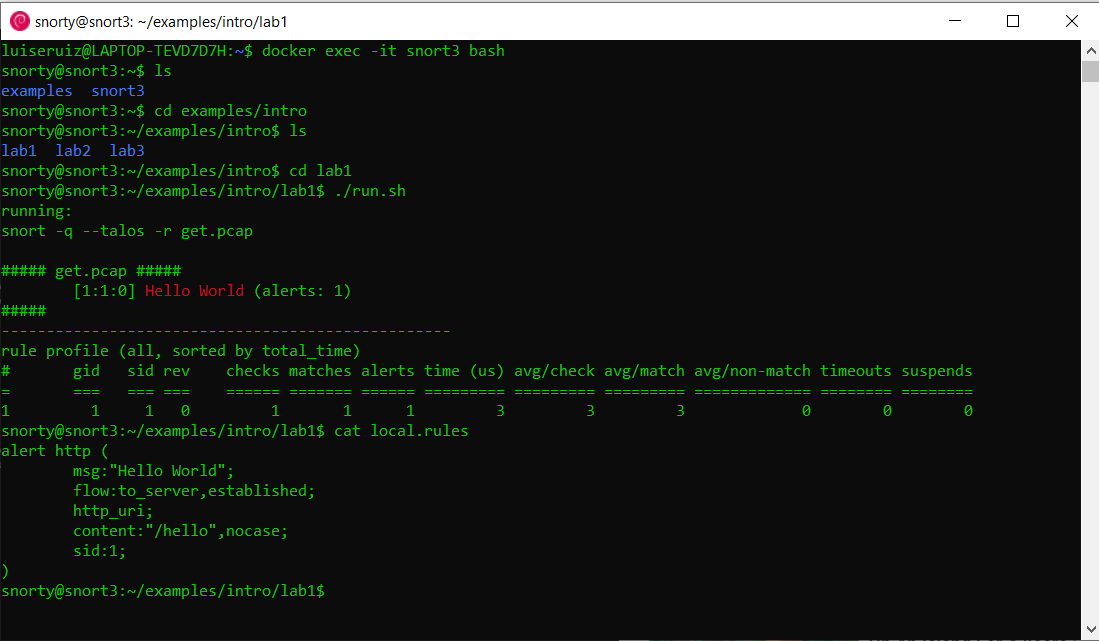
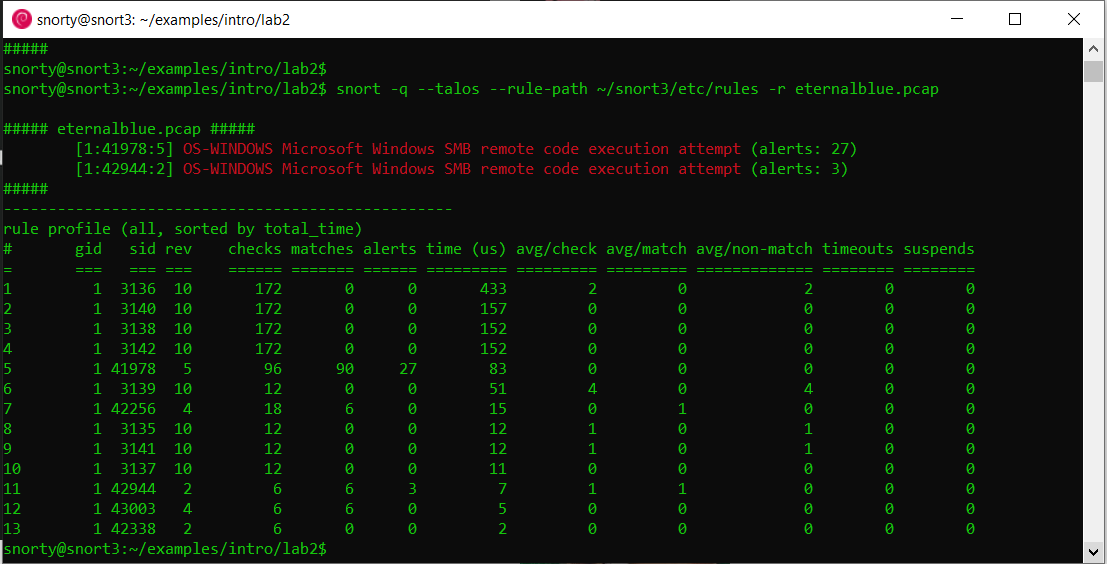


1. Now we will select the plan. Remember, since we have less than 250 employees and make less than $10 million a year we can use the free plan. This is backed up by Docker’s FAQ “Docker Desktop can be used for free as part of a Docker Personal subscription for: small companies (fewer than 250 employees AND less than $10 million in annual revenue), personal use, education, and non-commercial open source projects.”. We will select the personal plan and click “Continue with Free”. 
2. Go to your email and verify your account. 
3. You are now registered with Docker. You can click start for the tutorial or hit skip tutorial. It is recommended to start the tutorial then come back, we will skip it and proceed with the installation. 
4. We now need to make sure that we can enable integration with Debian (which we previously downloaded). Click on the white circle, this is settings, then click on resources and WSL integration. Make sure “Debian” is turned on, if you do not see this button refresh. If you do not see the button after refreshing then go back and make sure you followed all the steps. 
5. Now we will finally install Snort3. To do this, we will now open Debian, it has a red circle logo. Once it is open you will need to type in the following commands in order. The first command will begin to install snort3. The second command will assign it to a container and attach it to docker.
   1. Docker pull ciscotalos/snort3
   2. Docker run --name snort3 -h snort3 -u snorty -w /home/snorty -d -it ciscotalos/snort3 bash
6. You will now see the container in docker.

****

## Testing

Now we will begin testing Snort3. We will have two tests, one with internal rules and another with external rules. To start snort we will enter docker exec -it snort3 bash. 

1. Now we will begin testing snort. Once we are in it, we will type “ls” to see the files that came with it. There should be two files. Then we will change the directory to examples “cd examples/intro” then list the files “ls”. Now we will have three labs. We will go to the first lab and run it through the internal tool. “Cd lab1” then “./run.sh” . It will run then we should get only a single flag. 
2. To see what caused the flag we will type “cat local.rules” We will now see the message that caused this flag. 
3. Next we will test it with an external rule. “Cd lab2” to change directories. Then we will type in “snort -q --talos --rule-path ~snort3/etc/rules -r eternalblue.pcap”. We are directing snort to the external rule called eternal blue and we will run it through our file. We will now get many more alerts and it will give us information for what is causing alerts. 
4. Next we will close snort3 by typing in “exit” We have successfully installed Snort3 and tested it to make sure it can sniff packets using both internal and external rules!****

## Recommendations (Kari)

Snort is a powerful tool that can assist an organization in maintaining a secure network, however any tool needs to be well understood and supported to provide effective security. The Snort homepage provides a user manual, updated rulesets, and training. To effectively use this tool it is best the technician that works with snort understands the user manual, implements updated rulesets, and takes the training.

The Snort user manual is located on their website and discusses the installation, configuration and maintenance of the tool. If Snort needed to be updated or serviced, having the user manual available on hand would help expedite these processes and help mitigate misconfigurations of Snort. The user manual can be found at the following URL: <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>

The rulesets are the rules that outline abnormal behavior within the network. These need to be updated regularly and configured properly to ensure that the tool can effectively identify abnormal traffic. These rulesets can be found on snorts website at the following URL: <https://www.snort.org/search?query=1&submit_search=>

The Snort website also provides training resources and articles designed to help a user better understand how to use this tool. These training resources can be found on the snort website at the following URL: <https://www.snort.org/documents>

## Alternatives (Marcos)

Our security team identified Suricata as an effective alternative intrusion detection system. Suricata is a free open-source network threat detection engine that provides capabilities including intrusion detection (IDS), intrusion prevention (IPS) and network security monitoring. It performs well with deep packet inspection and pattern matching which makes it incredibly useful for threat and attack detection. While many of Suricata’s features mirror Snort’s, Suricata has notable distinctions; It’s multi-threaded so a single instance can perform at much higher traffic volumes. There is more support available for Application layer protocols and detection rules; for instance, it can identify HTTP or SSH traffic on non-standard ports based on protocols. Suricata supports Npcap for packet capturing, hashing and file extraction, and can be combined with the Lua scripting language, which can be used to modify outputs and even create complex and detailed signature detection logic. Once Ashburn’s frog emporium’s network has expanded its boundaries, Suricata would be a more appropriate service without compromising the network's performance.

# Veracrypt

## Information About Tool (Ryan)

VeraCrypt is based on an open source product called TrueCrypt. While TrueCrypt is no longer used due to its security weaknesses, VeraCrypt has become a leading on demand file encryption tool. VeraCrypt is an open source product meaning that there is no cost for an organization to obtain and use this tool.

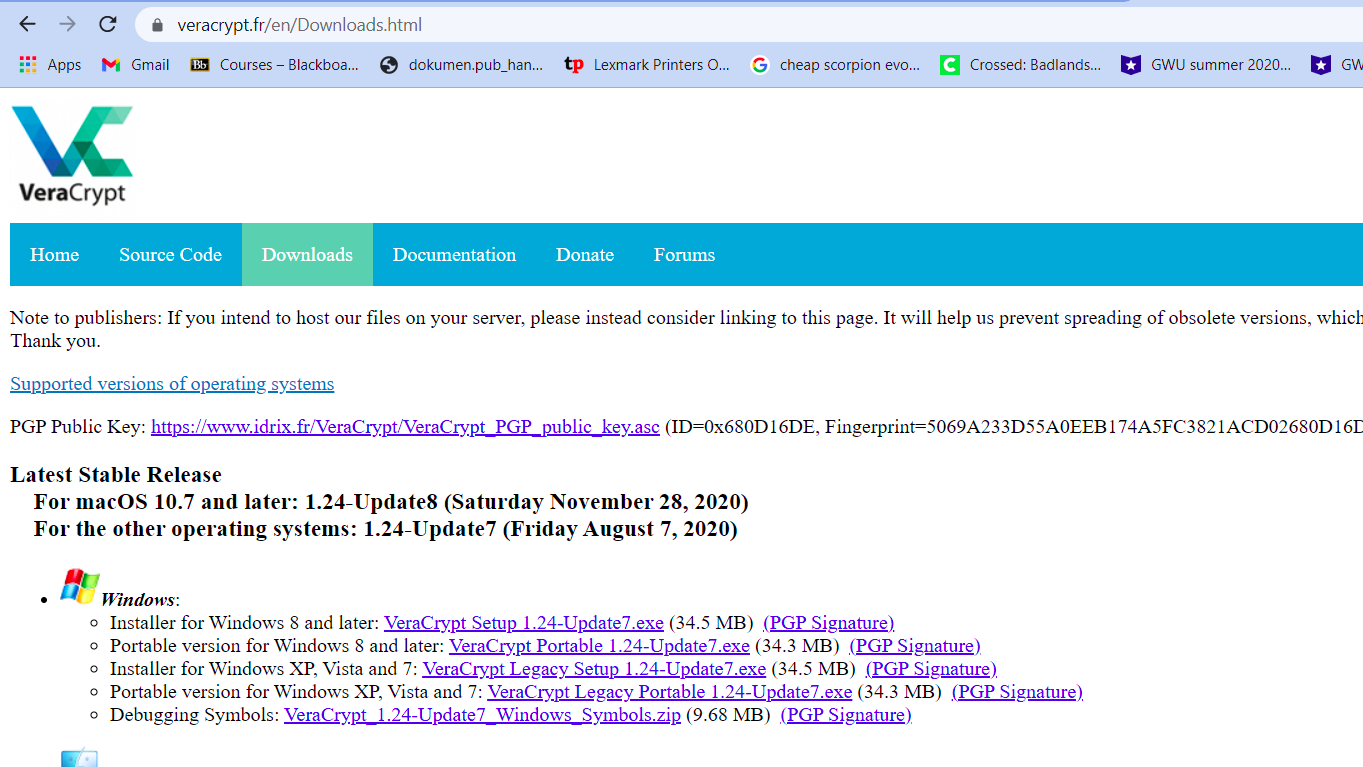
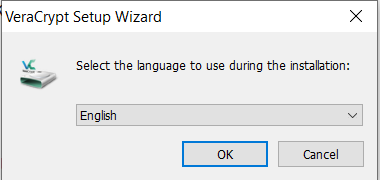
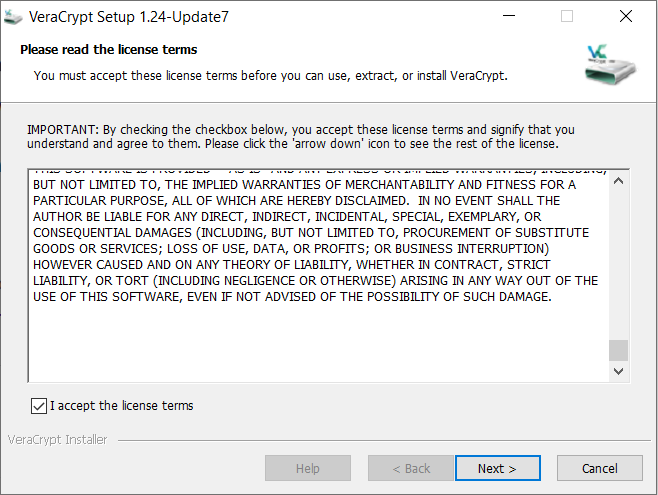
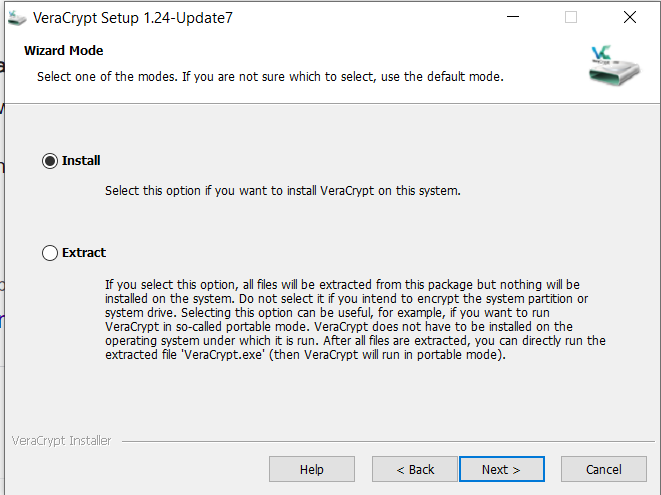
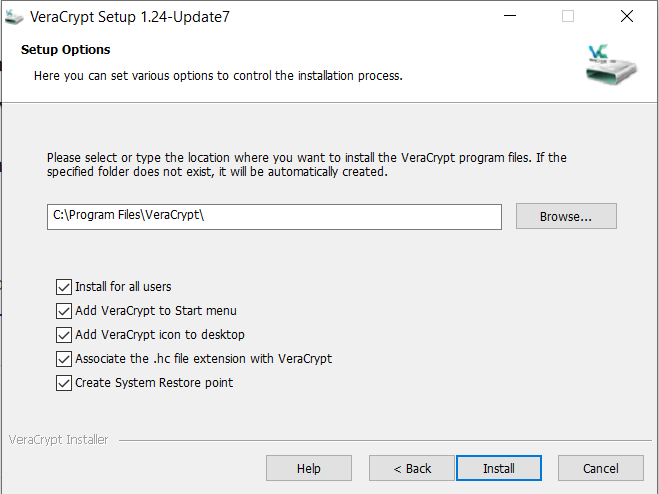
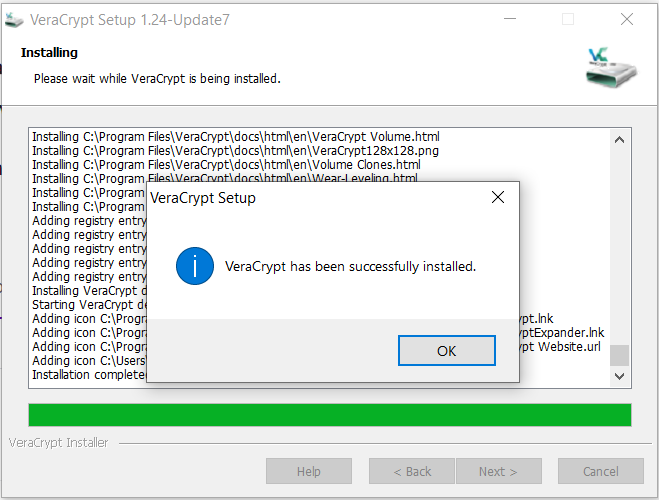
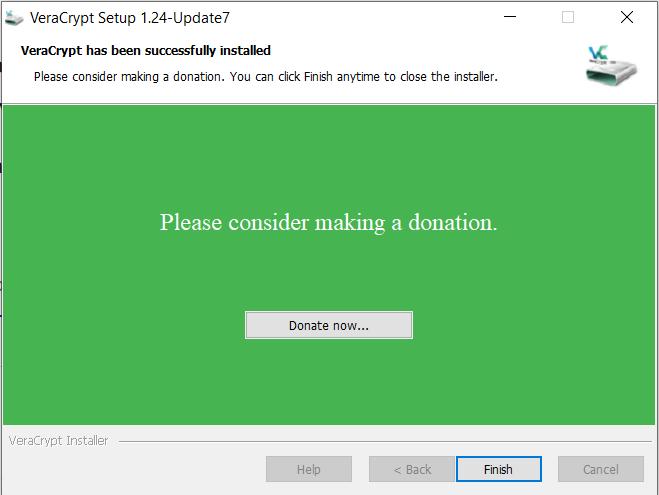
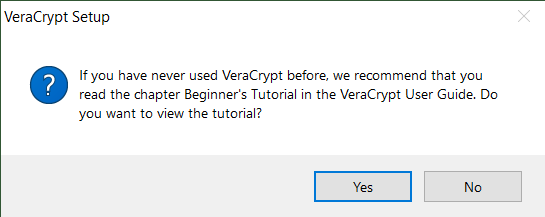
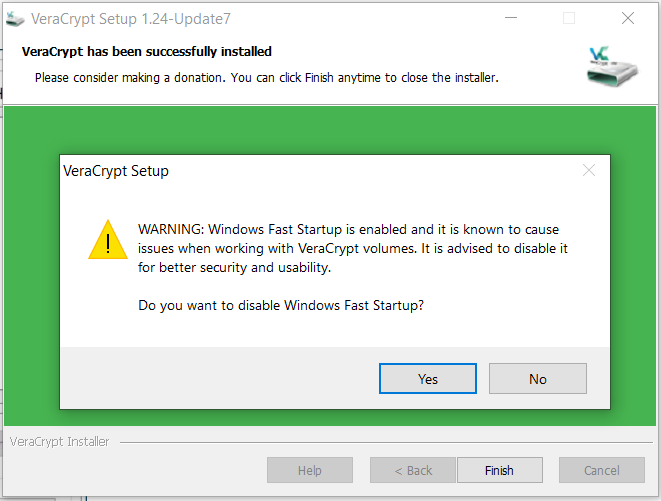
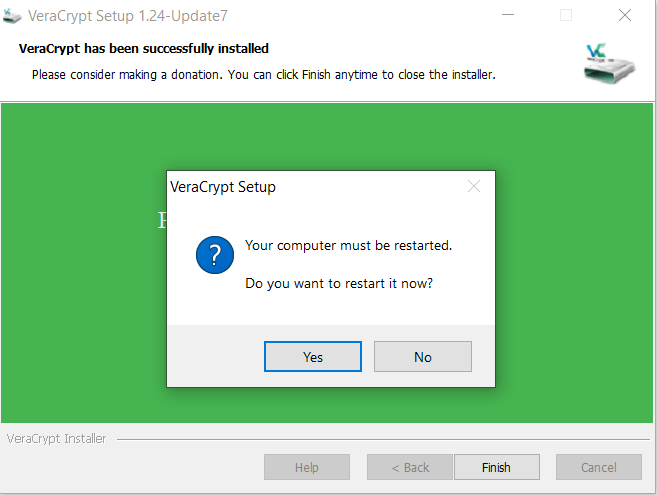
With access to numerous encryption methods, VeraCrypt is able to create encrypted virtual disks that work just as a standard disk would. Additionally, users are able to encrypt entire partitions for Linux machines. If a user is on a Windows operating system, then they are able to encrypt entire storage drives and other devices. Users can even hide volumes inside of other volumes, this means that if someone is able to mount the first drive, they would be unable to find the contents of the hidden volume. This is a key to providing data confidentiality for many organizations. VeraCrypt leverages Advanced Encryption Standard or AES for the tool’s primary encryption method, it does this through using AES with 14 rounds coupled with a 256 bit key. In addition to AES, there are three other Encryption algorithms that are used by VeraCrypt and those are Serpent, Twofish, and Cascades.

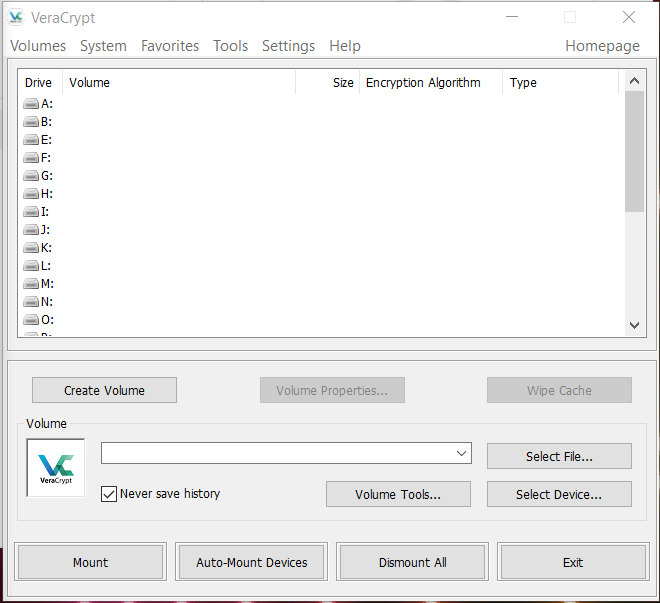
Furthermore, VeraCrypt allows for the combination of more than one algorithm. This comes into use when using VeraCrypt to create passwords for your encrypted containers. The VeraCrypt software will use one of five different algorithms that will produce three different outputs. These are the master key, the secondary key, and finally the salt. Three of the hashing algorithms that are used by VeraCrypt are RIPEMD-160, SHA 512, and Whirlpool.

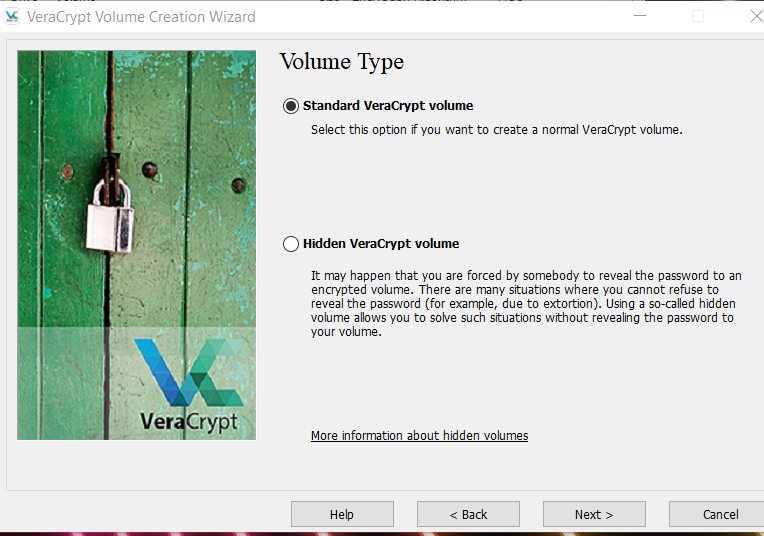
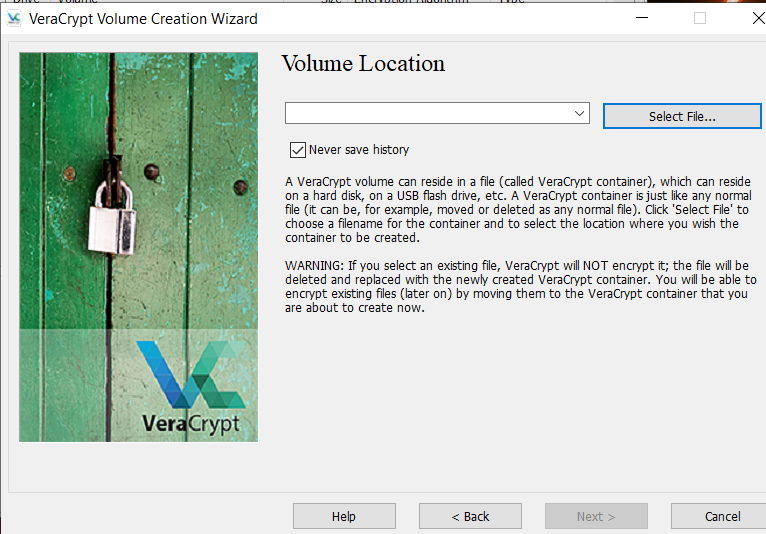
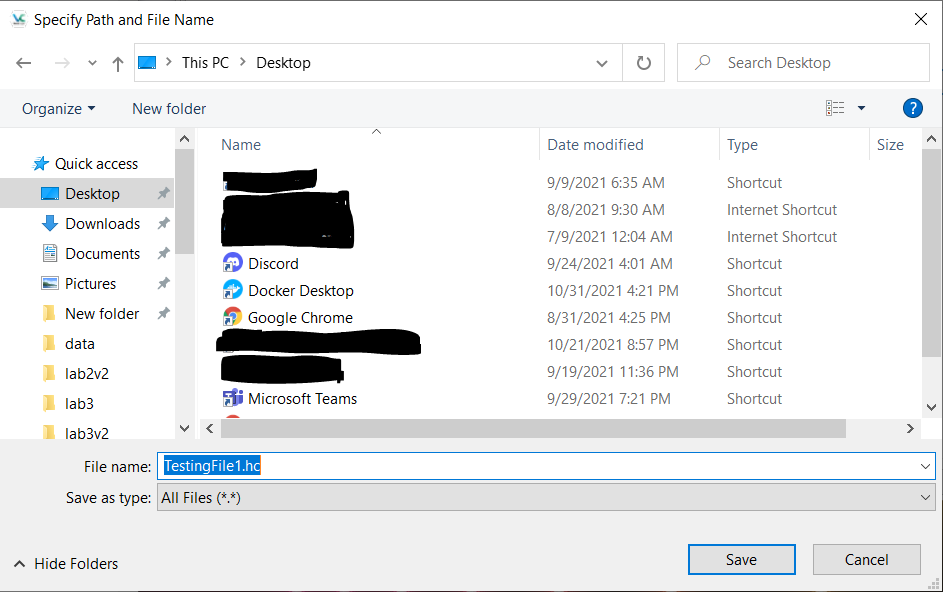
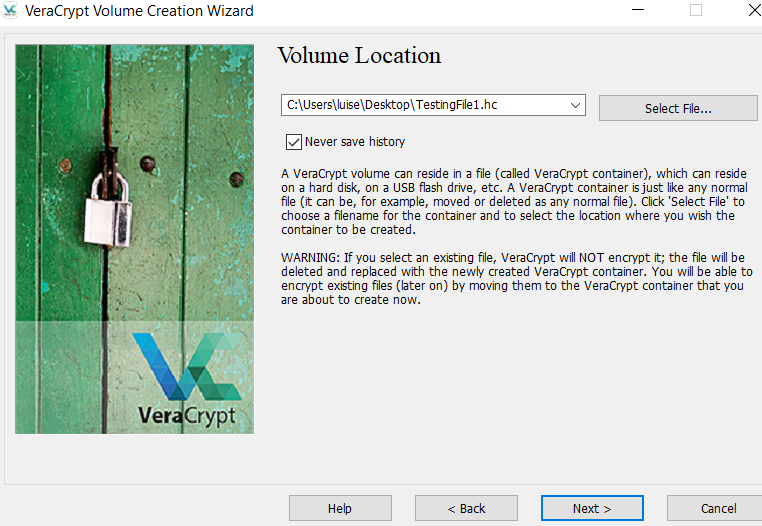
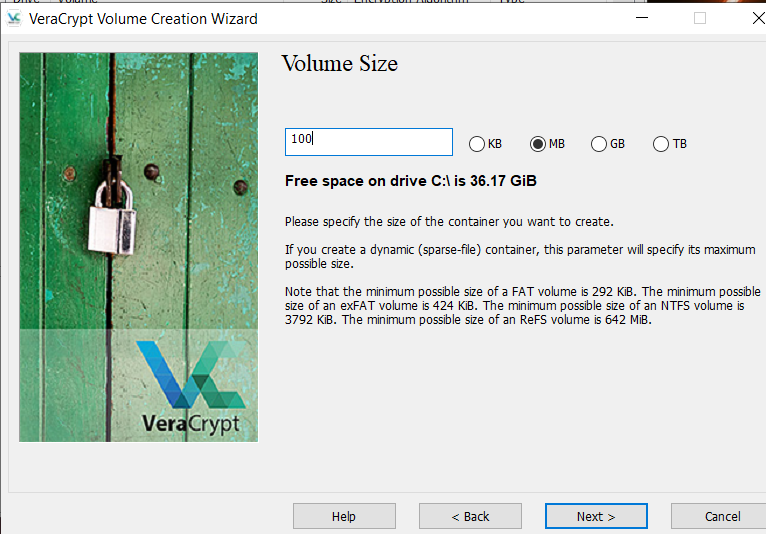
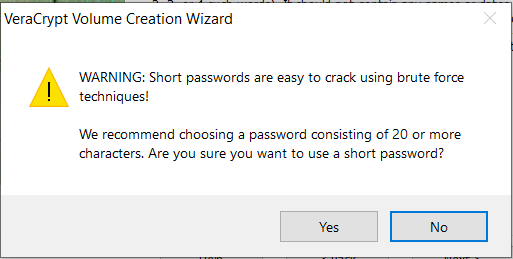
## Prerequisites

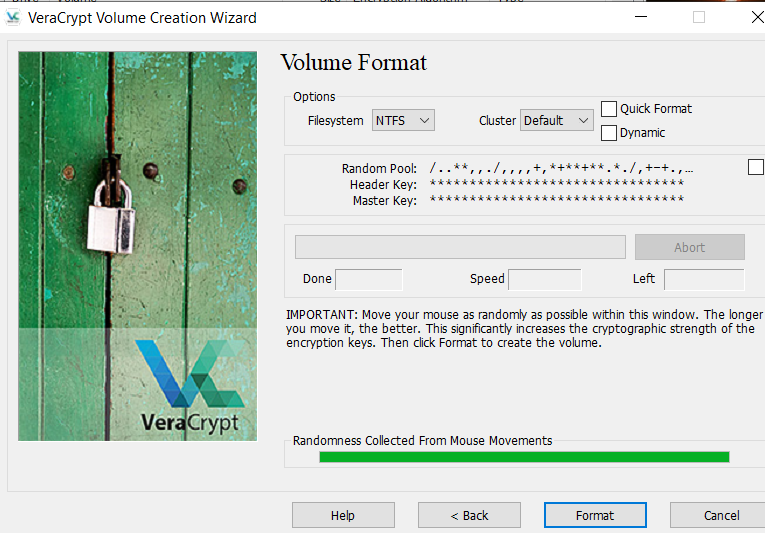
* VeraCrypt is supported by the following operating systems:
  + Windows 10
  + Windows 8 and 8.1
  + Windows 7
  + Windows Vista
  + Windows XP
  + Windows Server 2008 R2 (64-bit)
  + Windows Server 2008
  + Windows Server 2003
  + Mac OS X 10.9 Mavericks
  + Mac OS X 10.8 Mountain Lion
  + Mac OS X 10.7 Lion
  + Mac OS X 10.6 Snow Leopard
  + Linux (32-bit and 64-bit versions, kernel 2.6 or compatible)
  + Raspberry Pi OS (32-bit version)
* VeraCrypt has no memory requirement to operate this tool.
* At least 34.5 MB of local disk storage.

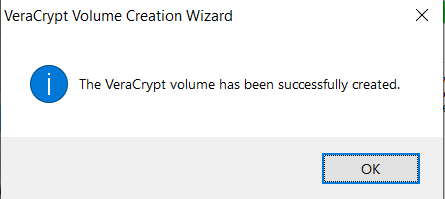
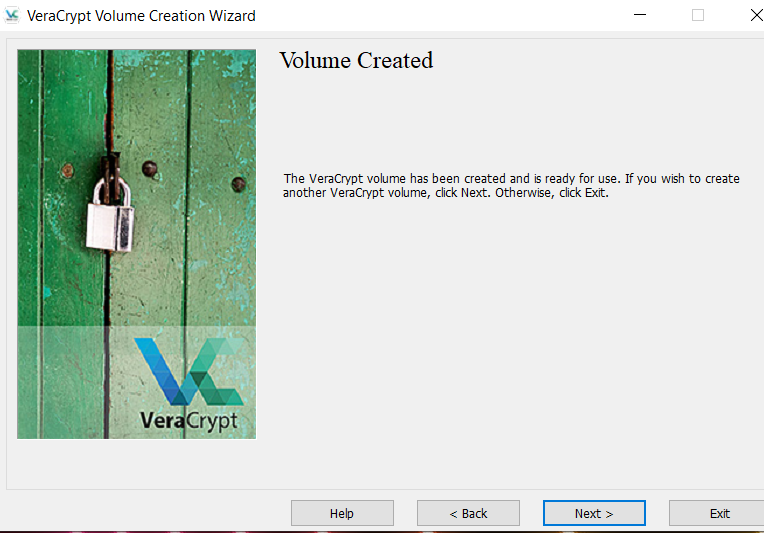
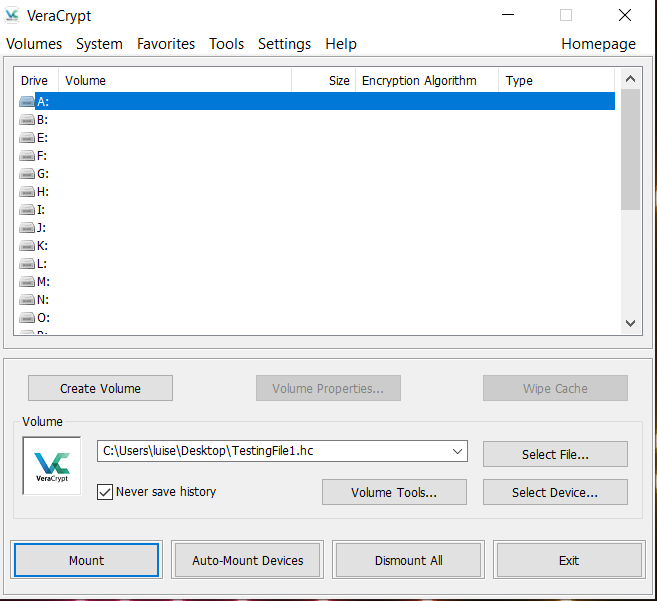
## Installation (Luis)

1. To begin with Veracrypt we will need to go to veracrypt.fr/en/Downloads.html. Download the option for the latest version, it should be the first option. 
2. This is how it should look like in your downloads menu
3. Select your English as your language and click okay. 
4. Read the License Terms, accept them and click okay. 
5. Click Install and Next
6. Choose where you want to install Veracrypt and choose all the options you want, in our case, all of them. Then click next. 
7. Once it has been installed click okay. 
8. Donate if you want to support Veracrypt, it is not required. Click Finish.
9. You will be prompted to read the User Guide. Since we will be going over most of it and more, it is not necessary but, it will help your understanding. Click No. 
10. Since fast startup causes issues with encryption and we want to avoid possible loss of data we will disable it. Losing encrypted customer and business records is too much of a risk compared to starting up the computer faster. Disable Fast Startup by clicking Yes.
11. Restart your computer by clicking Yes. 
12. Now we will create a volume. Open Veracrypt from your desktop. If not, search through your programs. Click “Create Volume”.



1. Choose, “Create an encrypted file container” then Next. 
2. Choose “Standard Veracrypt Volume” then Next 
3. Choose “Select a File” 
4. Create any name, in this case we used “TestingFile1” since we are only doing a simple installation then test. Save it to the Desktop. Click Save.
5. Review the name and location then Next.
6. Make sure you have “AES” and “SHA-512” Selected then Next. 
7. Since we are only using this as a test we are only selecting 100 MB however, choose more depending on the size of your file. 
8. Create a volume password that you will remember, in our case “P@$$w0rd”.
9. If your password is too weak it will ask you to create a longer one. We will continue because we will not be saving anything important to this volume yet. 
10. Choose the “NFTS” file system then move your cursor erratically until the bar becomes green. Then click format.

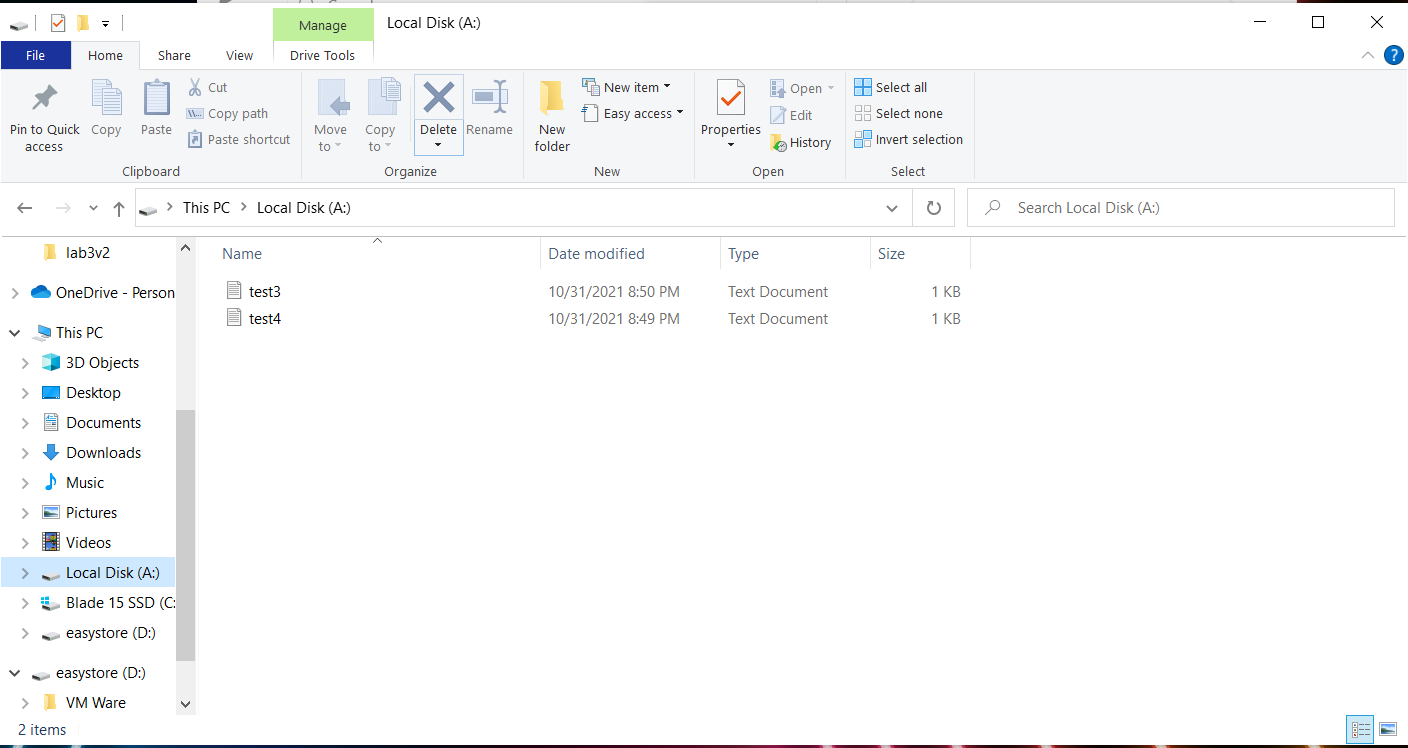
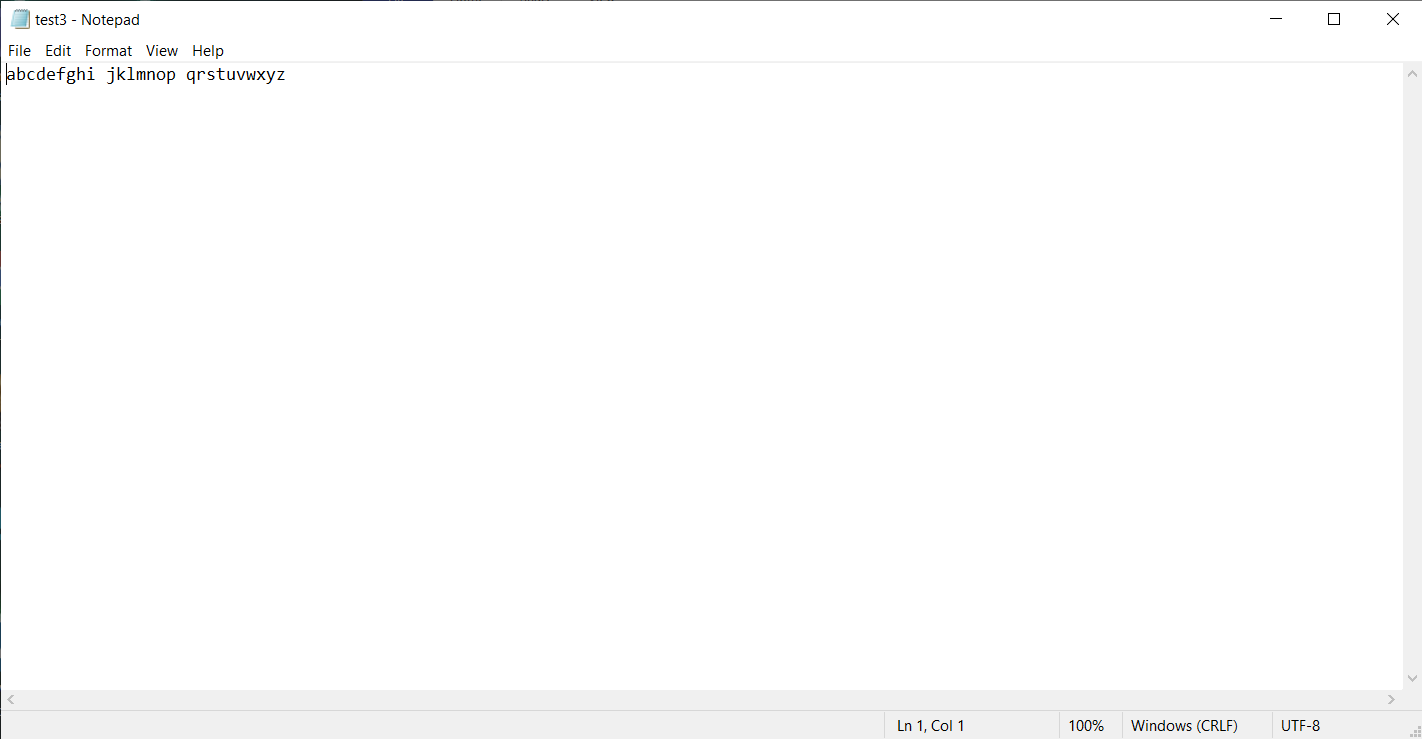


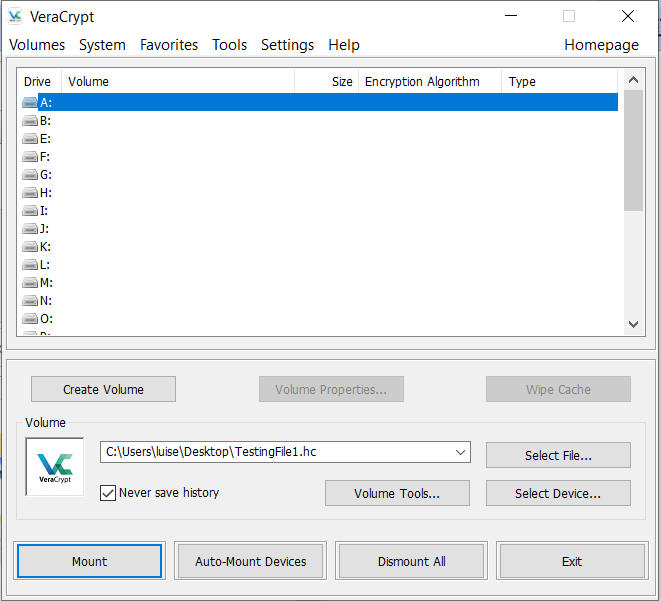
1. The volume was successfully created, click Okay. 
2. Another confirmation that it was successfully created. Click Next. 
3. Next we will mount the Volume to Veracrypt. While the Volume is mounted, all the files within it will be accessible through the disk location the volume is mounted on. It can be mounted on any letter but it will create a disk for that Volume in it’s mounted location. This will make more sense in practice. When the Volume is dismounted, all files within it will become inaccessible. Choose the Volume File we just created, click on a random letter and click Mount. 
4. You will be prompted to enter a password, enter the one that you just created for the Volume then Next.

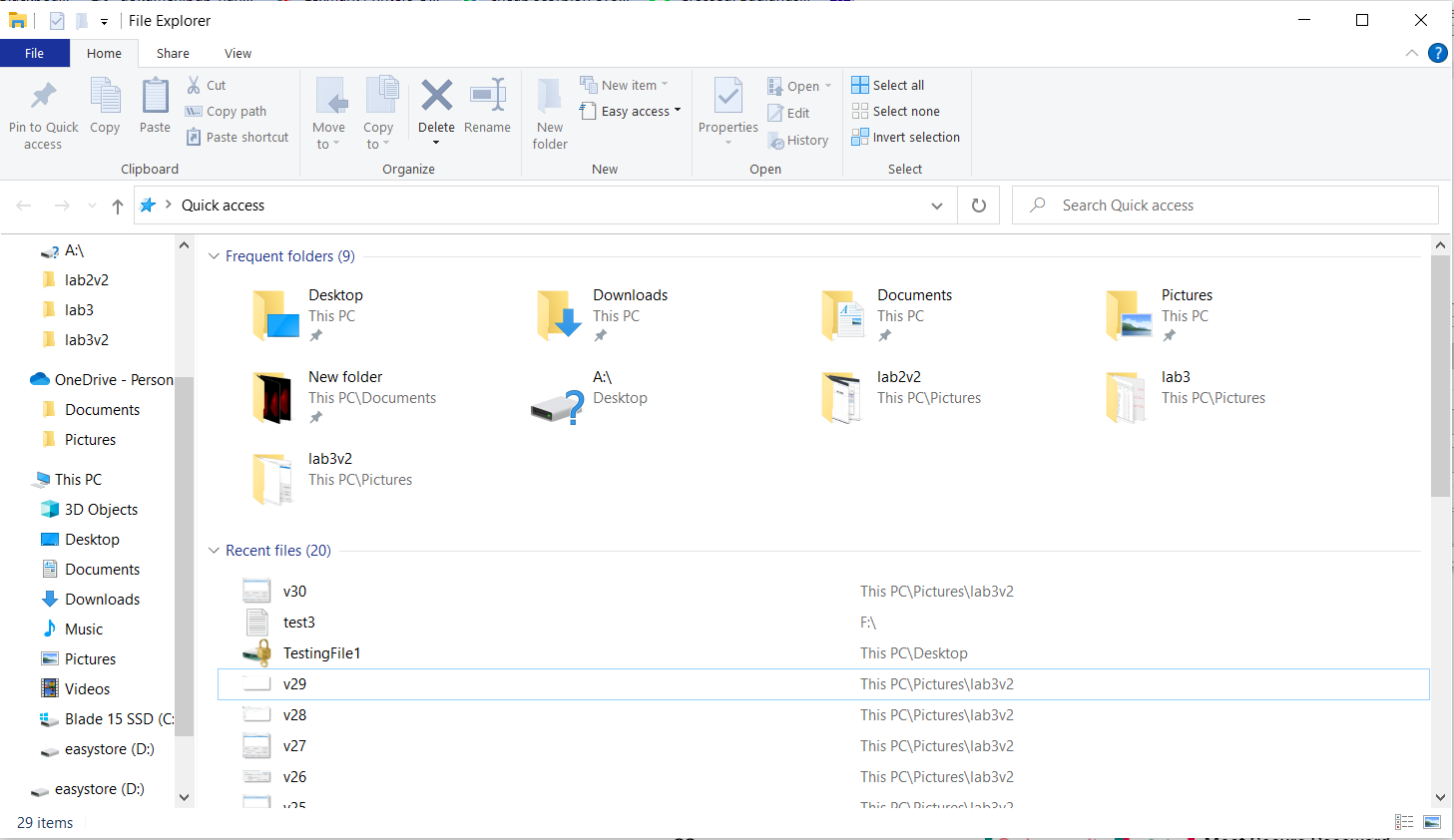


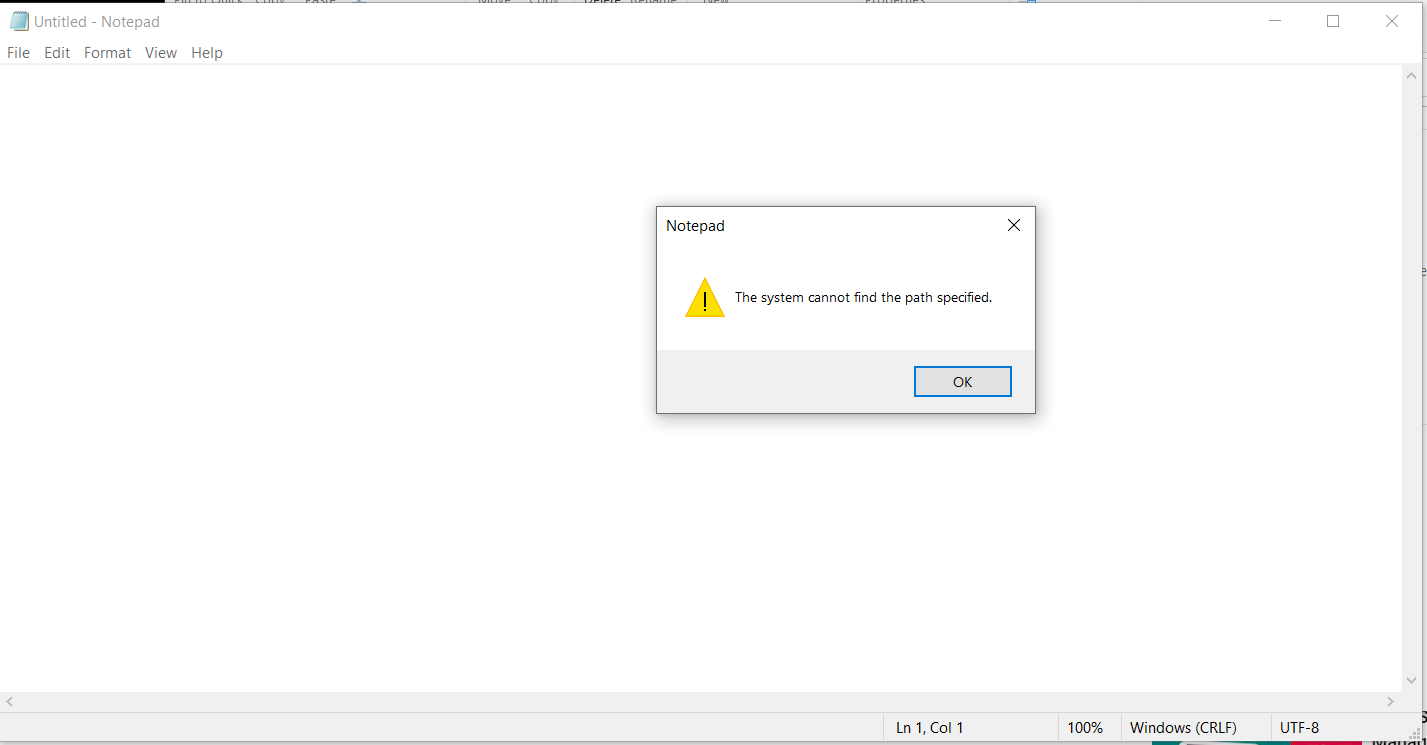
1. The Volume was successfully mounted. ****

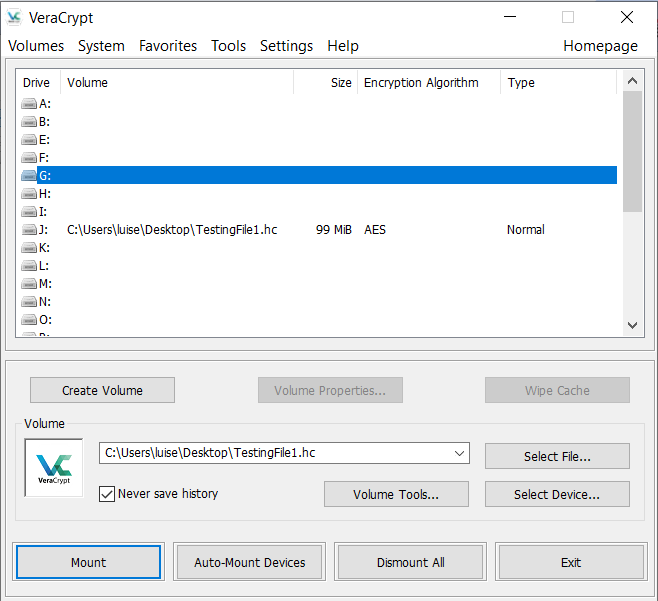
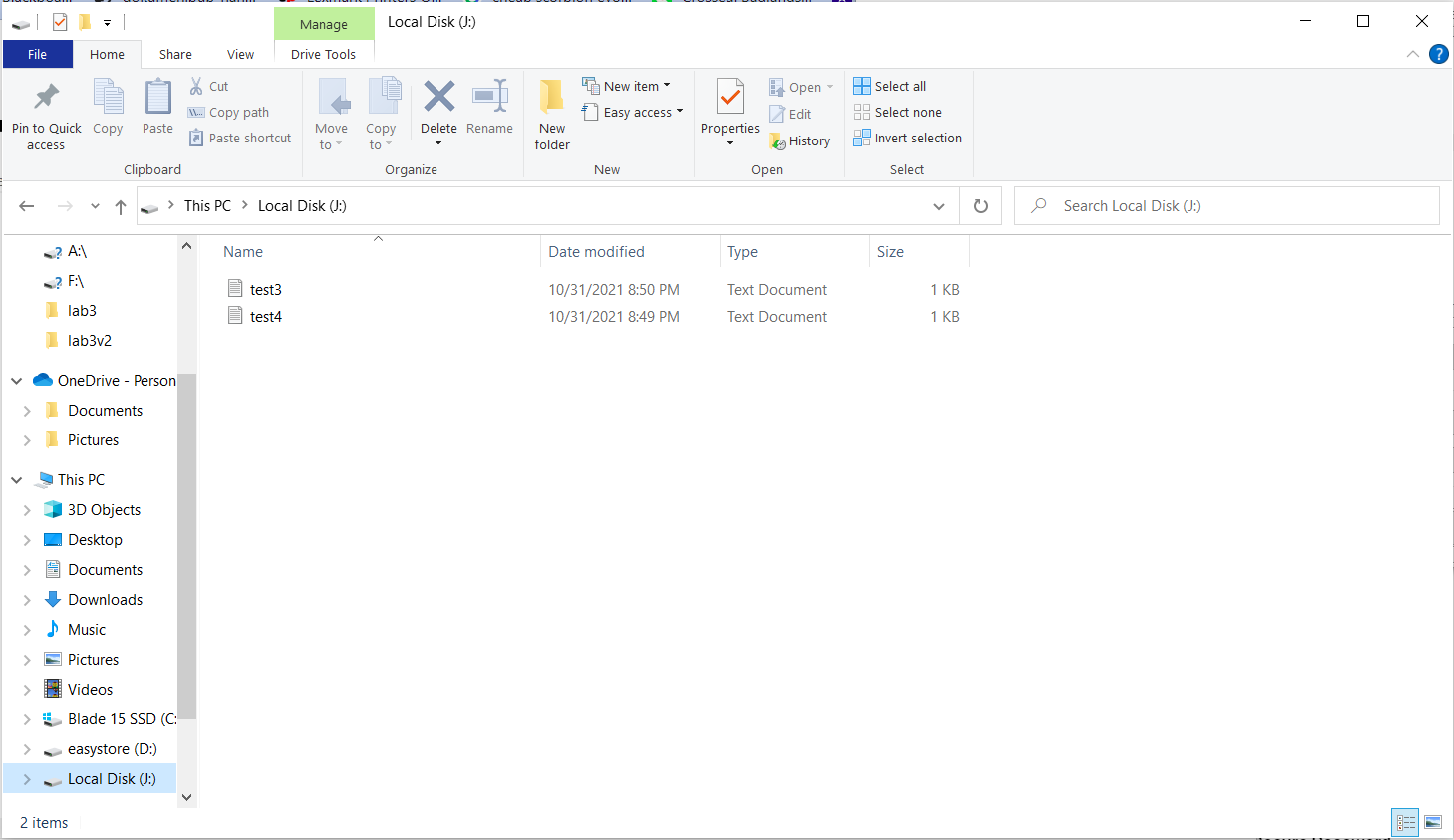
## Testing

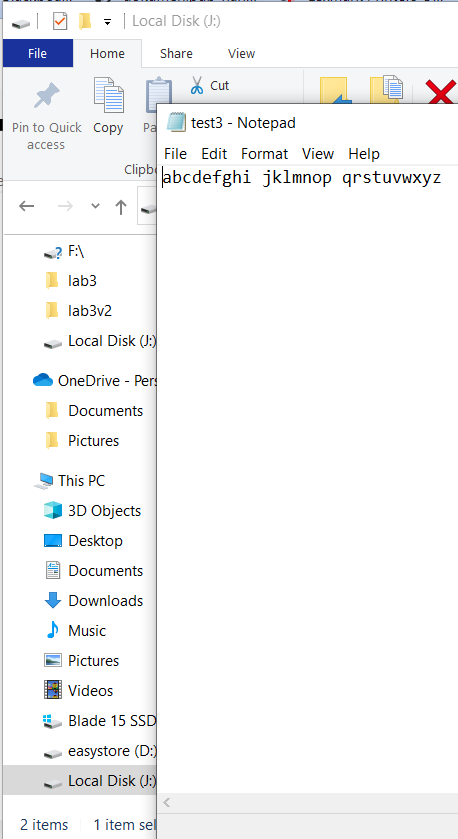
1. Now that the Volume was mounted we will create two notepads which are Test3 and Test 4. They do not contain anything important and will be used to demonstrate how files are encrypted. In the production environment make sure that you have carefully secured your Volume password to avoid important files being lost. 
2. This is what the files contain and what will be encrypted. 
3. With the Volume still mounted, click dismount. Now you will see that the Volume is no longer appearing on Veracrypt.



1. Look at the file explorer. You should notice that the “A:” drive is no longer there. What would happen if you try to open the “Test3” file? 
2. You will be unable to open the file once the Volume containing them has been dismounted. This is working as planned. If you can still open the file if the Volume has been dismounted then go back and make sure you have saved the file in the Volume. It should have been “Local Disk (“Your letter”:)”.



1. Next, we will mount the Volume to another letter. It does not matter, we are mounting it to “J:” just to demonstrate this fact. If you need further instruction with mounting, go back to Step 25. 
2. Open File explorer and now you will see that “Local disk (J:)” has been created. What will happen if you try to open the “Test3” file now? 
3. The file will now open and display the same data as previously. If it is not opening make sure that you tried to open the correct Volume container.



1. If the “Test3” and “Test4” files did not open when the Volume was dismounted but mounted when the Volume was mounted then Veracrypt is working as planned. You can now encrypt important files by moving them into volumes then dismounting that volume when not in use. It is VERY important that you do not lose or forget your password so make sure that it is something you will remember, but hard to crack and or make sure you write it down somewhere only you would be able to access it.

## Recommendations (Kari)

Veracrypt is a powerful local encryption tool that creates a password protected container for files on a local device. This is designed to provide a secure depository for sensitive files. With any secure system, it is only as secure at the password protecting it. Additionally, a tool is only effective if properly used. We recommend that a password policy be established as well as the technician that uses this tool reviews the user guide.

Passwords need to be kept secure to ensure that data is secure. We encourage to support a strong password for containers that all passwords fit within these parameters:

* A minimum of 8 characters
* At least one lowercase letter, one uppercase letter, one number, and one special character
* Passwords are updated once every 3 months

When a tool is used, it is essential that a user manual is easily accessible. This allows a user to have a guide for troubleshooting as well as train new users on the tool. This information can be found at the following URL from the Veracrypt website:<https://www.veracrypt.fr/en/Documentation.html>

## Alternatives (Marcos)

Our security team at Ashburn’s Frog Emporium has identified Cryptomator as an alternative to VeraCrypt on the fly encryption software. Cryptomator is a free, open-source encryption tool to protect data with end-to-end encryption. It is a simple tool for digital self-defense that allows protection of cloud data. Most cloud providers encrypt data only during transmission or they keep the keys for decryption for themselves. These keys can be stolen, copied, or misused. Cryptomator works by creating a virtual drive through which the encrypted contents can be displayed, edited, and augmented. The vault, which is the encrypted data, can be located on any storage media connected to the computer, such as a local drive, network drive or USB flash drive. This tool is designed especially for use with cloud synchronization services such as OneDrive. With Cryptomator, we alone would have the key to the entire cloud data of Ashburn’s Frog Emporium. Cryptomator allows you to access your files from all your devices. It's easy to use and integrates seamlessly between your data and the cloud. The open-source program protects the data by meeting the latest standards and encrypts both files and filenames with AES and a 256-bit key length. To start with Cryptomator, you only need to assign a password for a folder within your cloud. The password assigned is never sent across the internet. Rather, it’s used to generate key files, which will authenticate you locally. Cryptomator never syncs your files and has zero-knowledge of your master password or vault contents. To access the vault, simply enter the password again. You will be provided with a virtual encrypted drive to which you can move your data, similar to a USB flash drive. Every time you store something on this drive, Cryptomator encrypts the data automatically. As Ashburn’s Frog Emporium expands to multiple locations, this would require more protected mobility to secure critical data. With Cryptomator, its unique and open-source encryption software will allow us to encrypt important data files before uploading it to the cloud.

# Conclusion (Kari)

Ashburn’s Frog Emporium is interested in improving their information security and has hired our security team to design and implement an integrated defense in depth method. This is designed to provide fault tolerance to the security tools implemented and ensure each aspect of the network is protected. We implemented Snort and Veracrypt into Ashburn’s Frog Emporium’s network. Snort is a powerful network monitoring tool that monitors the network for abnormal behavior. Veracrypt creates secure depositories for sensitive data to be encrypted and password protected. The implementation of these tools will reduce the amount of time an attack would occur and prevent the sensitive data from being read by an attacker.

# References

*"Features"*. Suricata. (2021, August 24). Retrieved October 31, 2021, from https://suricata.io/features/.

*"Why snort 3?"*. Snort Rules and IDS Software Download. (n.d.). Retrieved October 31, 2021, from https://www.snort.org/snort3.

*"Free open source disk encryption with strong security for the paranoid"*. VeraCrypt. (n.d.). Retrieved October 31, 2021, from https://www.veracrypt.fr/en/Home.html.

*"Install Docker Desktop on windows"*. Docker Documentation. (2021, October 28). Retrieved October 31, 2021, from https://docs.docker.com/desktop/windows/install/.

Lowen, C., Wojciakowski, M., Atif Ali, M., Coulter, D., Calvin, M., Satran, M., Gangapersaud, M., Nikolić, A., Raj, T., & Turner, R. (2021, October 5). *Manual installation steps for older versions of WSL*. Microsoft Docs. Retrieved October 31, 2021, from https://docs.microsoft.com/en-us/windows/wsl/install-manual#step-4---download-the-linux-kernel-update-package.

ciscotalos. (2020, January 30). *ciscotalos/snort3*. Docker Hub. Retrieved October 31, 2021, from https://hub.docker.com/r/ciscotalos/snort3.

Bricata. (2020, October 28). *What is suricata ids?* Bricata. Retrieved October 31, 2021, from https://bricata.com/blog/what-is-suricata-ids/.

Siemons, F. (2021, January 27). *Open source ids: Snort or suricata? [updated 2021]*. Infosec Resources. Retrieved October 31, 2021, from https://resources.infosecinstitute.com/topic/open-source-ids-snort-suricata/.

Flibledish. (2015, April 4). *Cryptomator: App Reviews, features, Pricing & Download*. AlternativeTo. Retrieved October 31, 2021, from https://alternativeto.net/software/cryptomator/about/.

Roach, J. (2021, September 26). *Cryptomator Review - updated 2021*. Cloudwards. Retrieved October 31, 2021, from https://www.cloudwards.net/cryptomator-review/.