**Name: Yilake Mengstie**

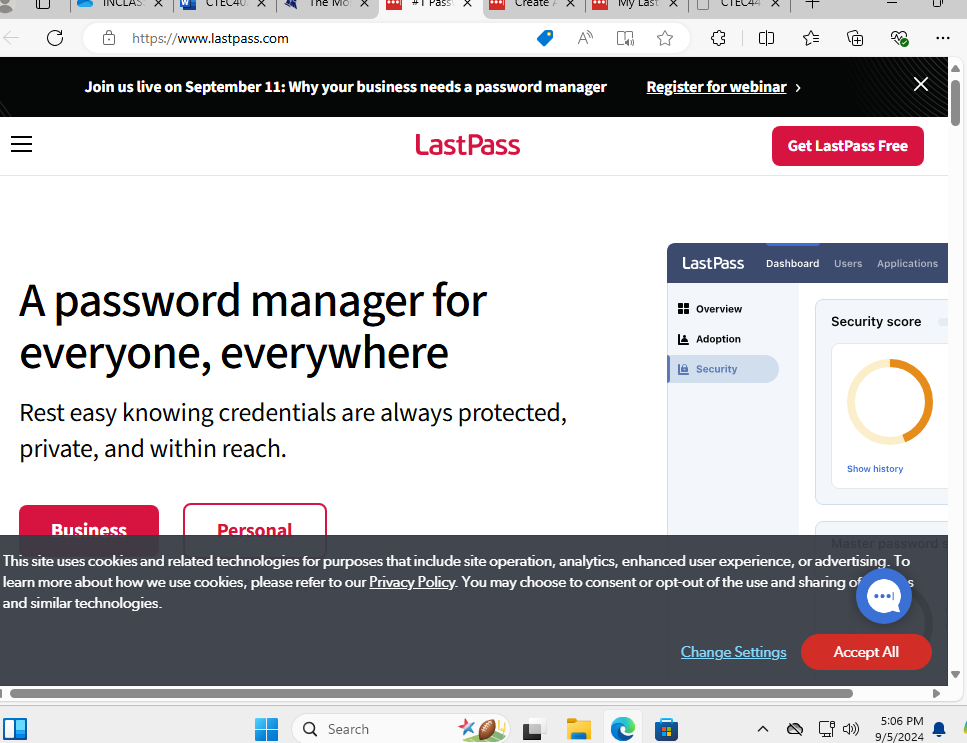
**CTEC402: In Class\_ Assignment3**

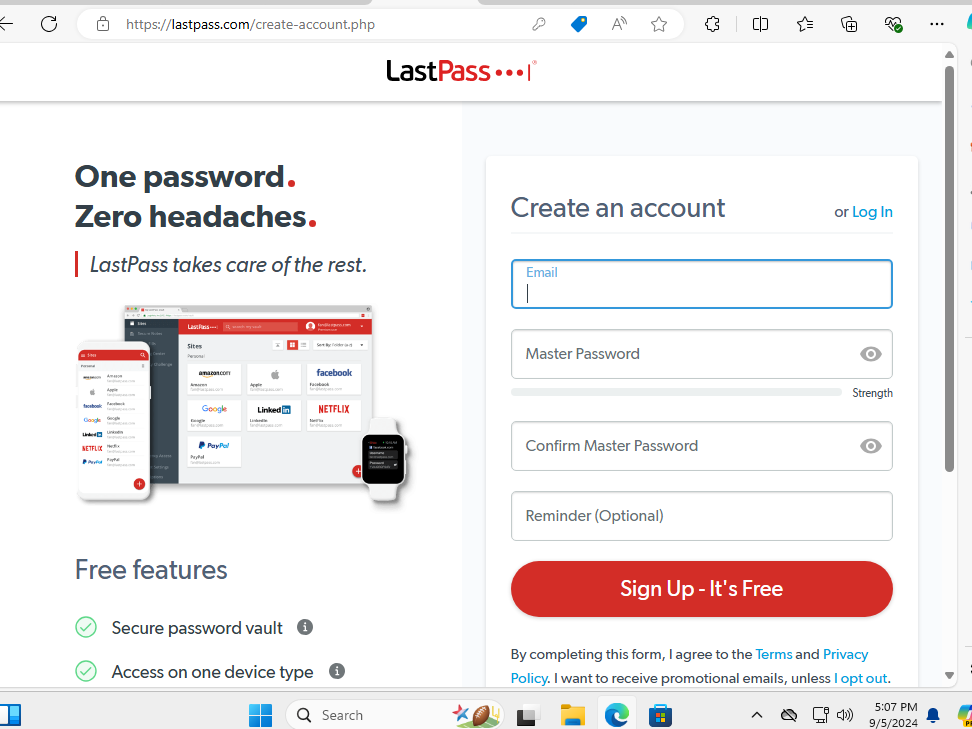
**Date; September 05/2024**

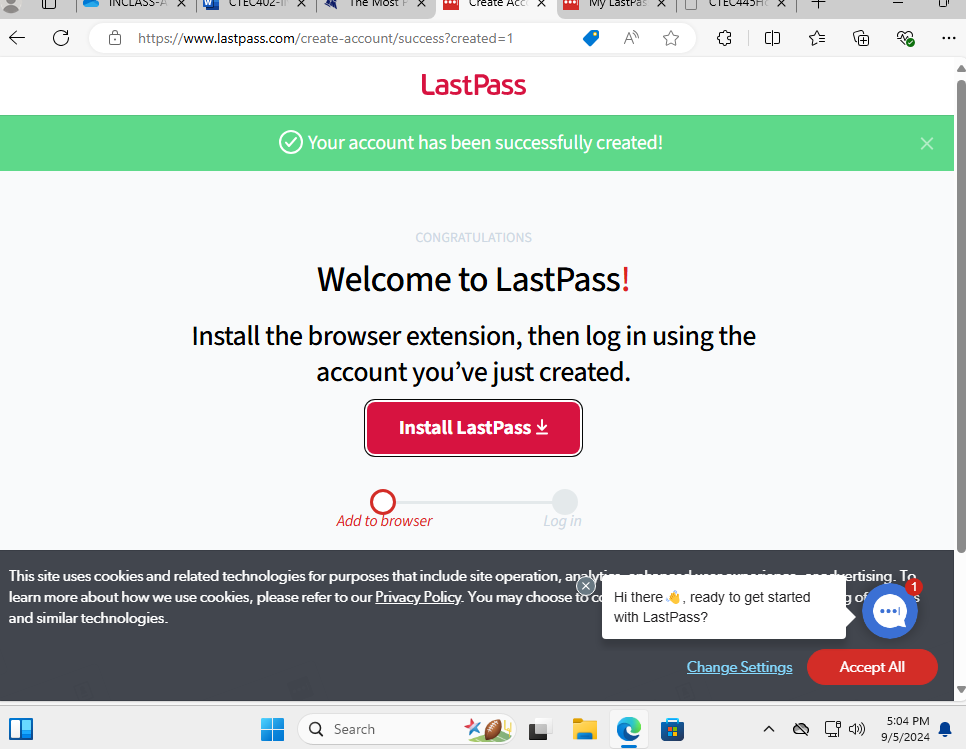
**Part 1: You need Explore the software’s (5 points)**

You need download at least 3 different Encryption Software and create step-by-step. documentation how did you encrypt. The most Popular Free Encryption Software Tools to Protect Your Data https://heimdals1. ecurity.com/blog/free-encryption-software-tools/

1. **LastPass**

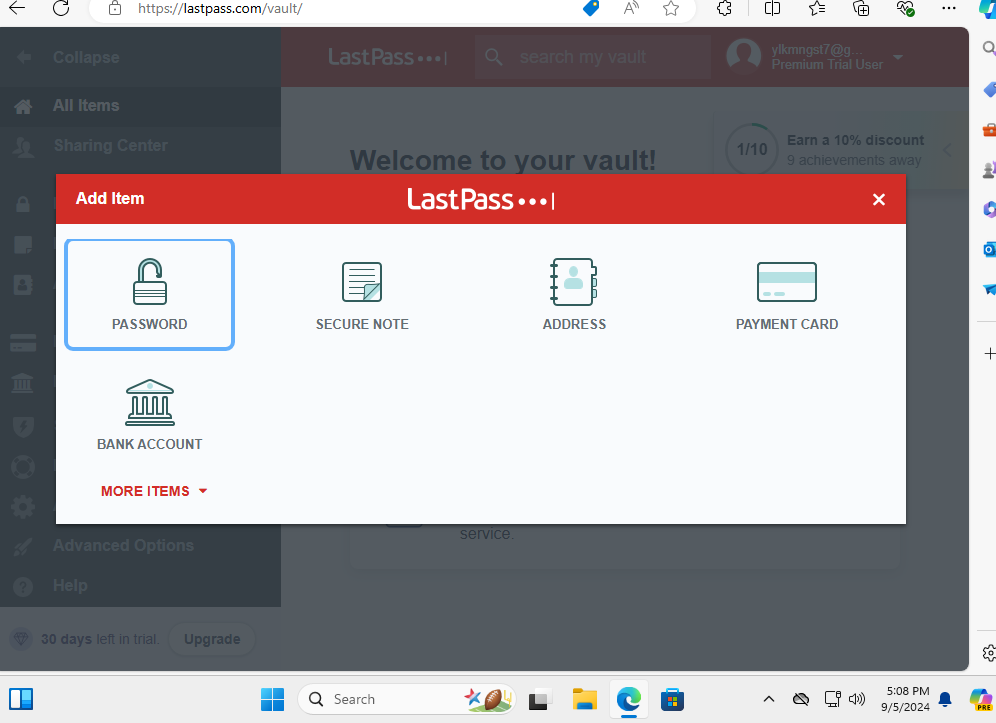
Step1: **Go to the official website**

**Step 2: create account** 

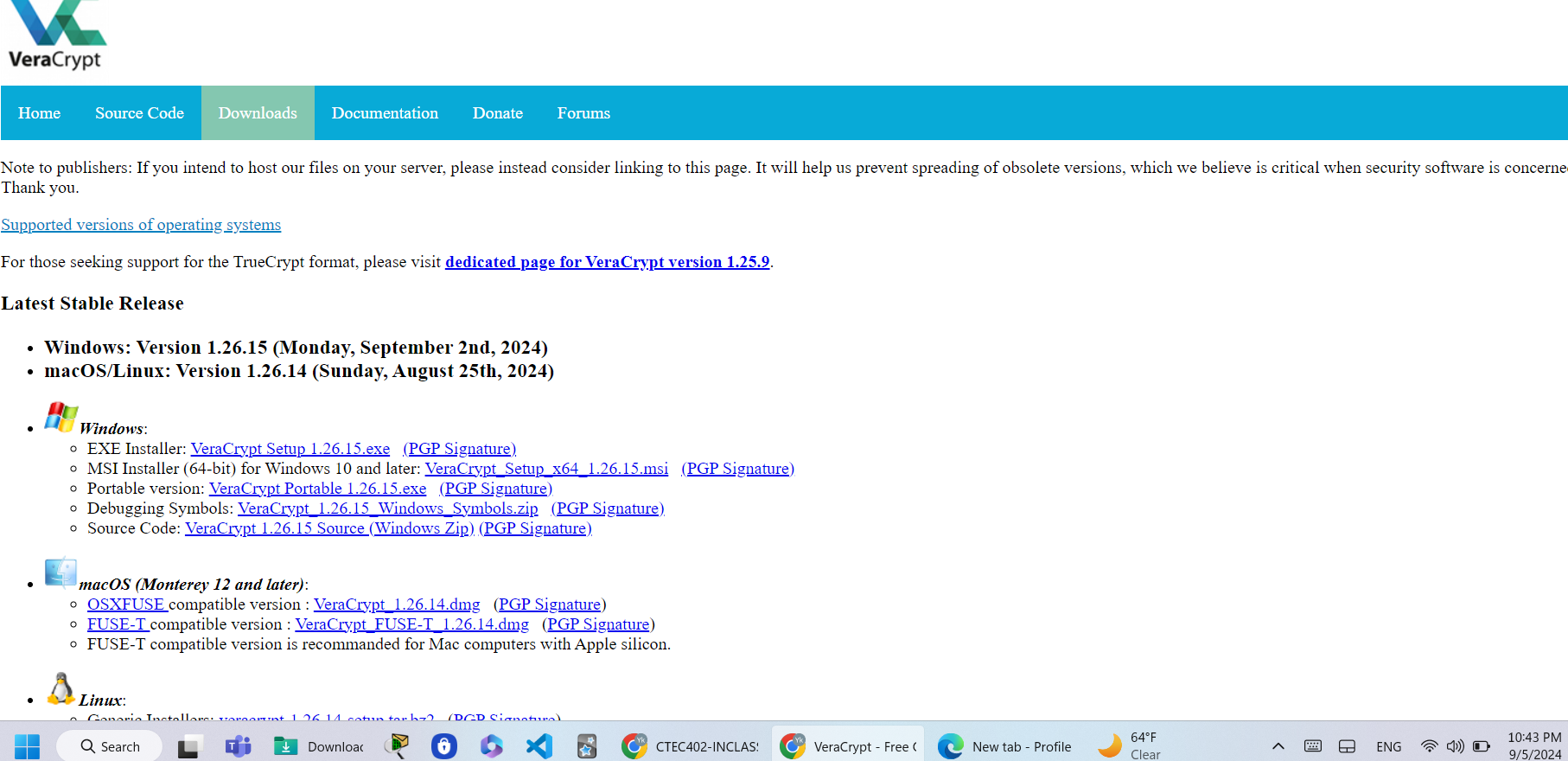
**Step 3: Shows LastPass Downloaded Successfully**  

**Step 4: Welcome window**

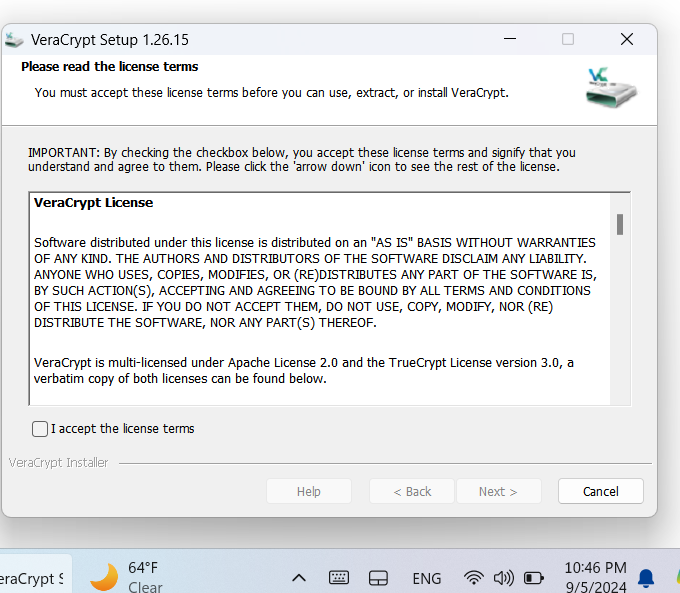


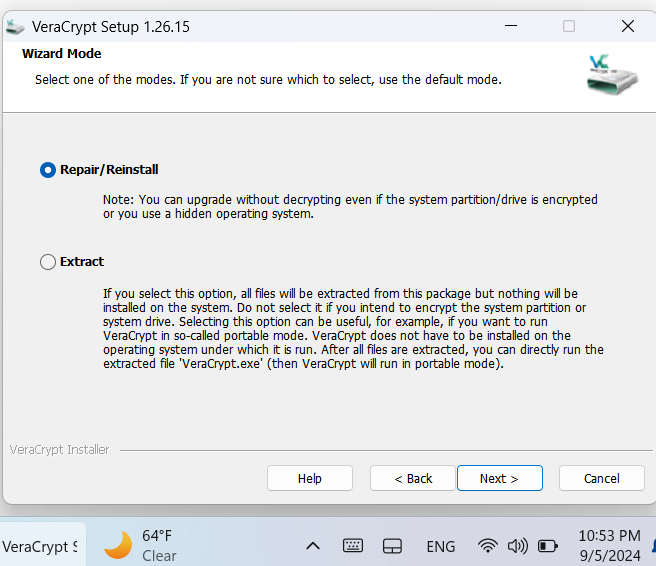
**Step 4: Click the “Add your password “button to add password.**  

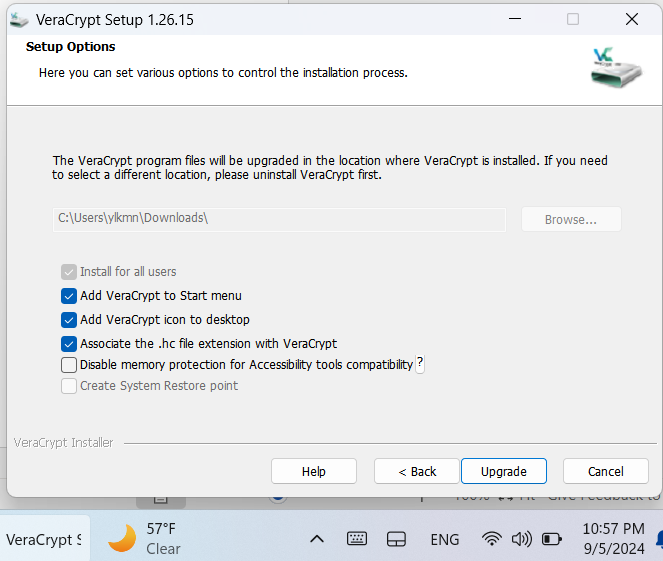
1. **VeraCrypt**

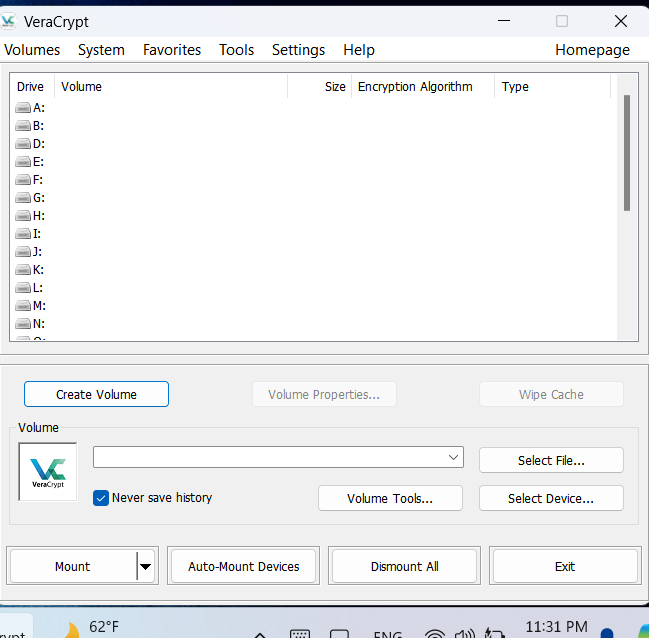
**Step 1:** Go to its official website 

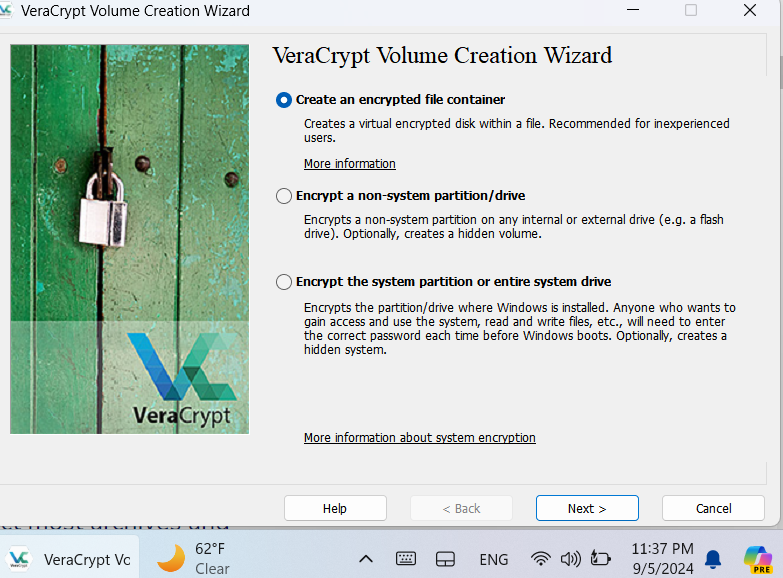
**Step 2: Run and accept software agreements**

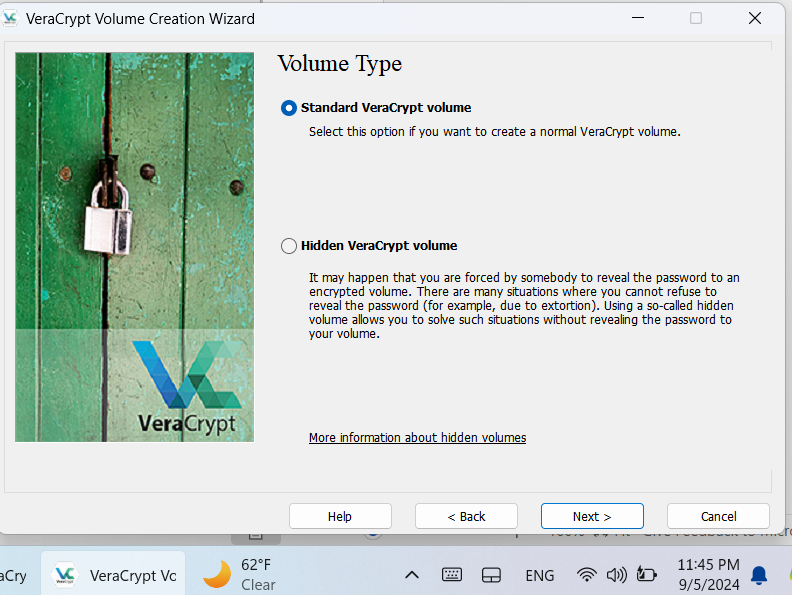


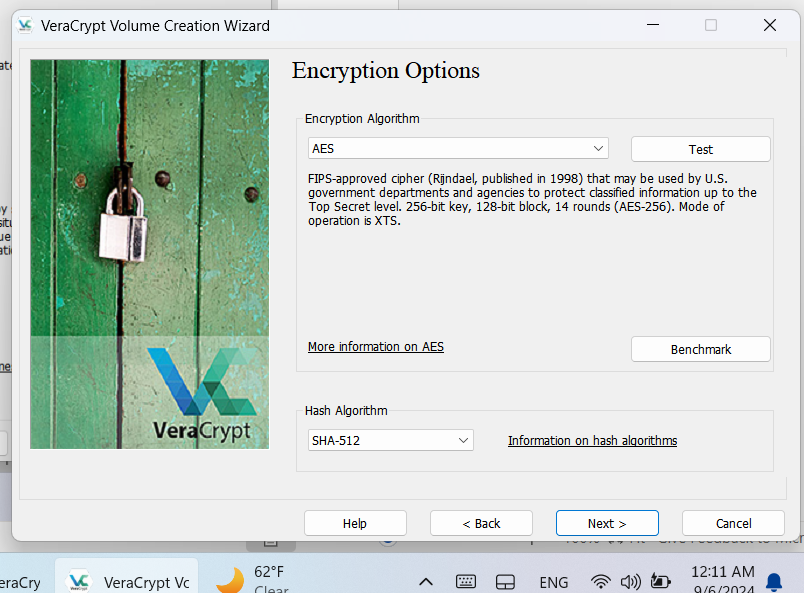
**Step 3: select the wizard Mode** 

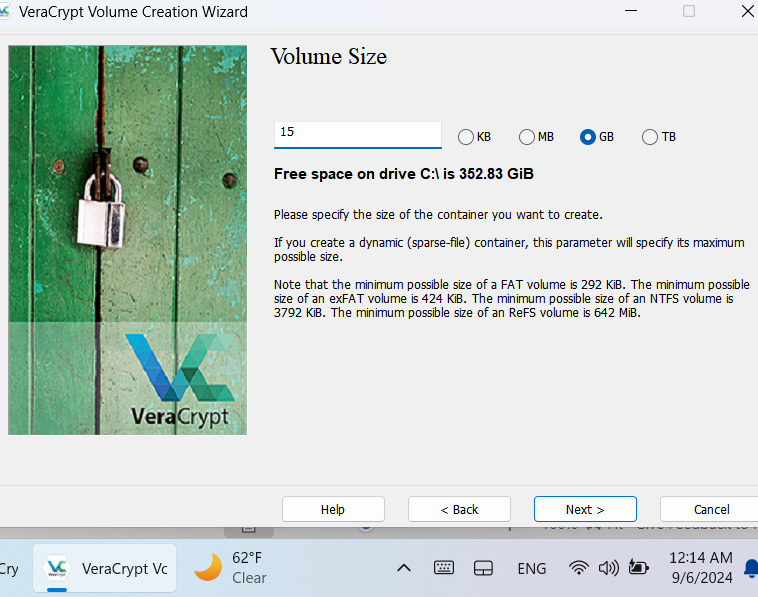
**Step 4: Select The Setup Option** 

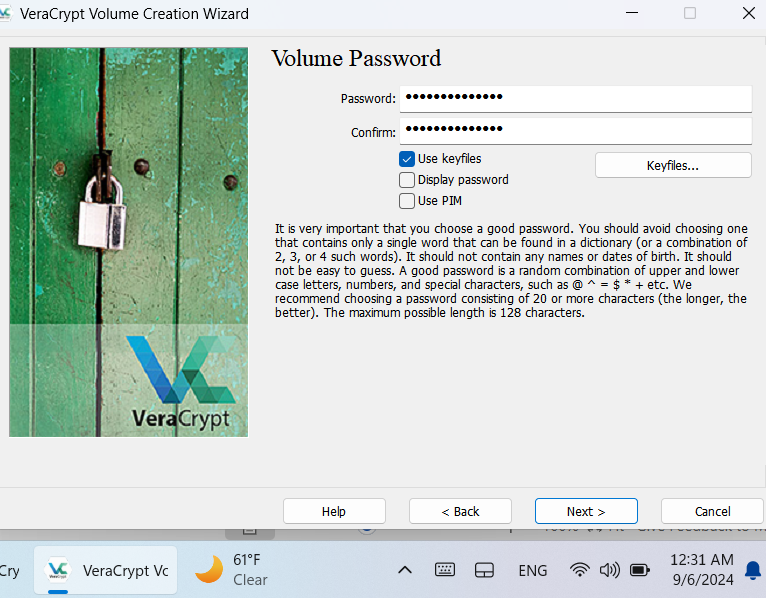
**Step 5: After VeraCrypt Successfully Downloaded Open It and Click The “Create Volume" Butto**n 

**Step6: Choose An Encrypted File Container** 

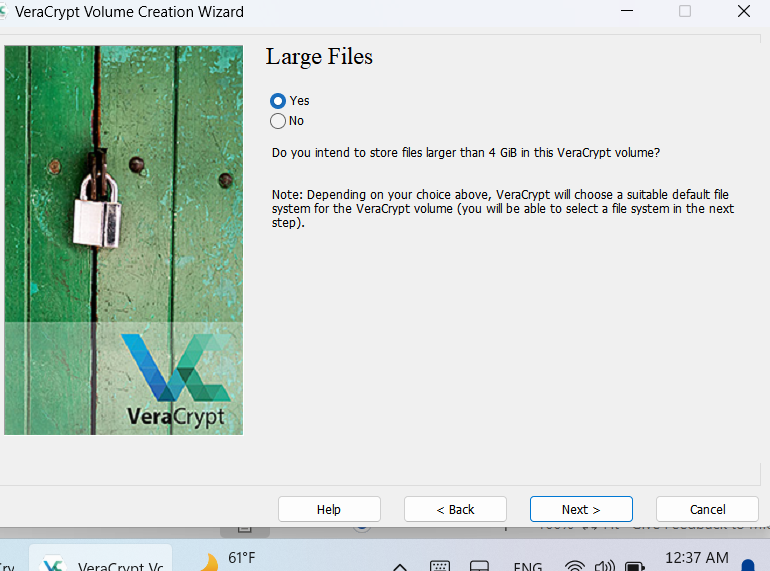
**Step7: Choose Volume Type from the Available Options** 

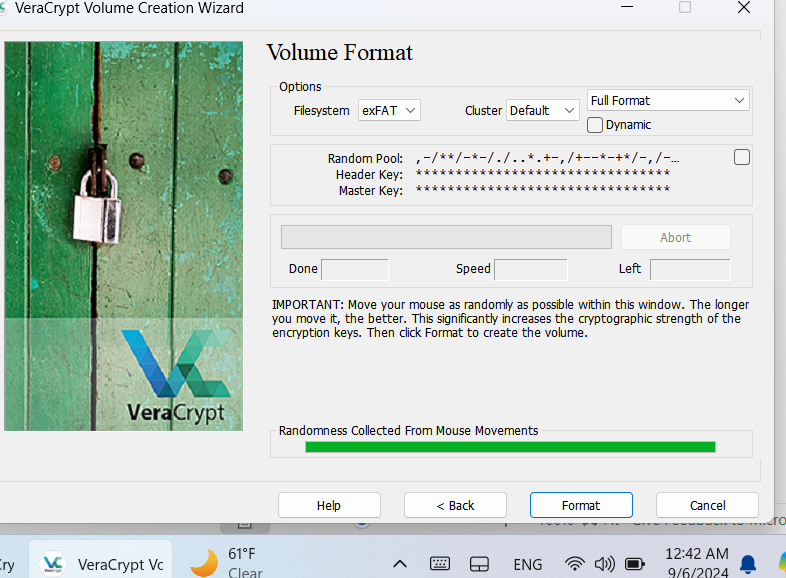
**Step 8: Choose Encryption Option** 

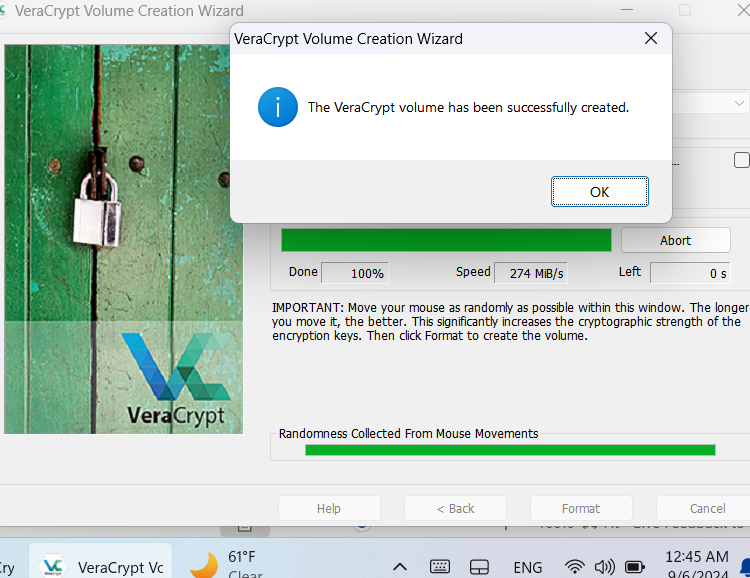
**Step 9: Set the Volume Size Based on How Much Data We Want to Store** 

**Step 10: Volume Password Set up** 

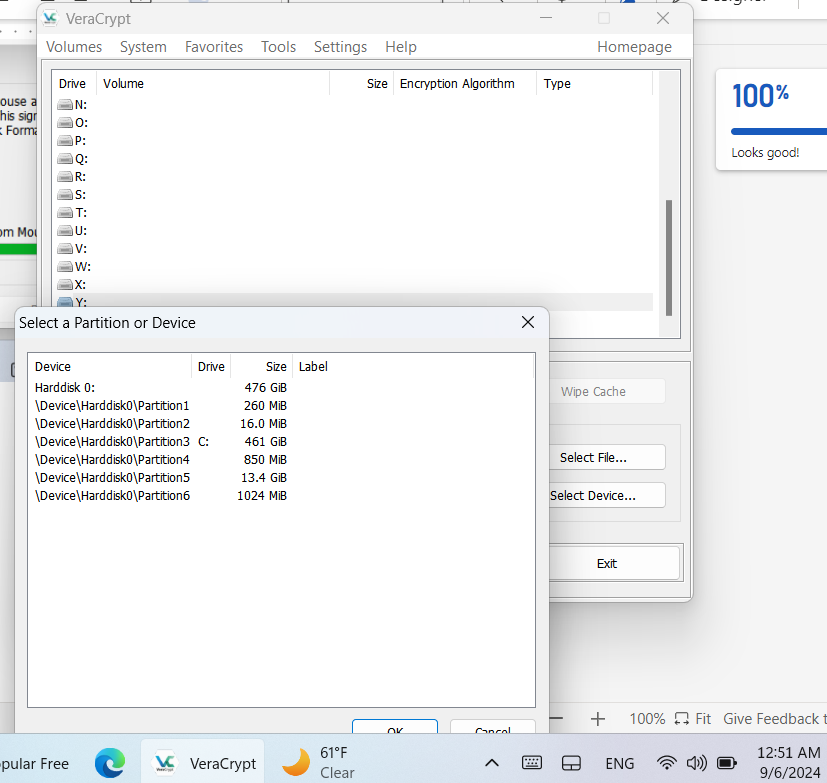
**Step 11: Chose File Size that Meet Our Interest**

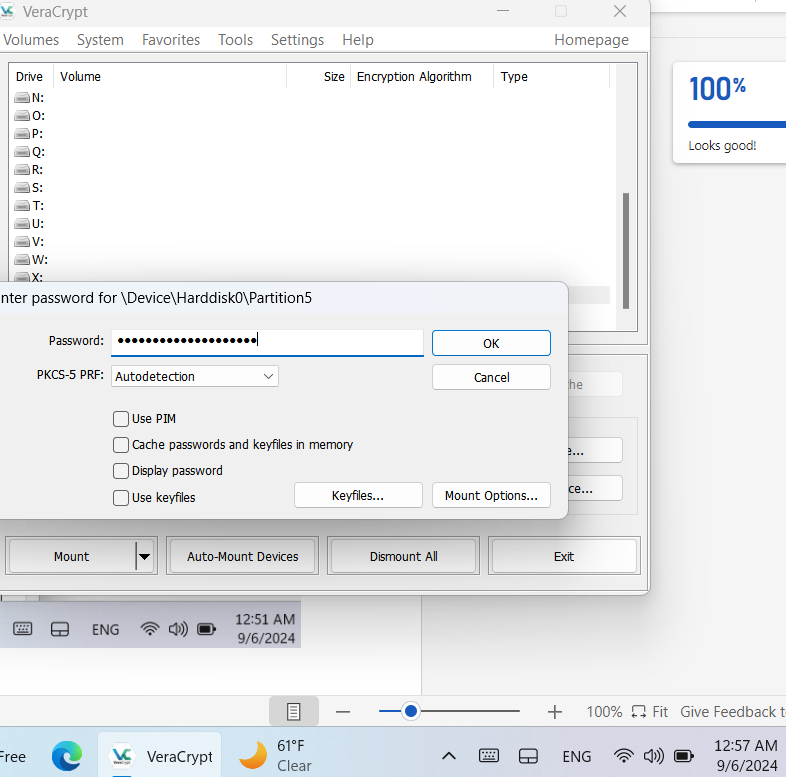


**Step 11: Format Volume** 

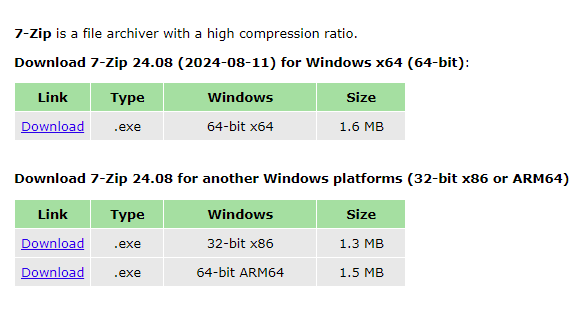
**Step 12: VeraCrypt Volume successfully created** 

**Step 13: Select Device letter and click “select Device” Button**

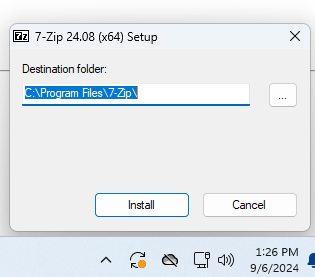


**Step 14: Mount The Disk** 

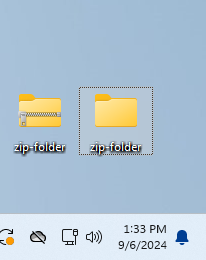
1. **7-ZIP**

S**tep 1: Go 7-zip official website and download the file** 

**Step 2: select the destination and click install**



**Step 4: create sample folder and zip, right click on it >compress to > zip fil**



**Part 2: Explain the following questions and how to recover encrypted files without password (2 points)**

First write your OWN words. Next, using the new AI ChatGPT, ask it the same question(s) and edit the responses down to 100 words.

**Part2.1 (1 points)**

1. How to Encrypt Files on Your Computer

**Answer**: We can use free or built-in tools to encrypt files and folders on our computers. For example, Windows operating systems, except for home versions, support BitLocker, which we can use to secure our documents.

**ChatGPT**: To encrypt files on your computer, start by using the built-in encryption tools that your operating system offers. On Windows, you can use BitLocker to encrypt entire drives or EFS (Encrypting File System) for individual files or folders. On macOS, you can use File Vault for full disk encryption or encrypt files individually using Disk Utility.

1. What Are the Benefits of Encrypting Sensitive Files on Your Computer?

**Answer:** The primary purpose of encrypting our sensitive data is to keep it secure and block any unauthorized attempt to access it. If hackers access our data, they can do anything on our behalf, and that activity puts our lives in danger.

**ChatGPT:** Encrypting sensitive files on your computer offers several important benefits. It protects your data by ensuring that unauthorized users cannot access or read your files without the correct encryption key or password, enhancing both privacy and security. This is especially critical for sensitive information like financial records, personal documents, or confidential business data.

1. What files do you need to encrypt?

**Answer:** We can encrypt any data, such as files, folds, and images, that we want to make secure. More importantly, susceptible data, such as social security numbers, Day, financial-related data, and others that, if they are accessed without consent, put our lives at risk. Those kinds of data should always be encrypted, including in storage or transmission.

**ChatGPT**: You should encrypt files that contain sensitive, personal, or confidential information to ensure they are protected from unauthorized access. This includes financial records such as bank statements, tax documents, and any files with credit card or investment details. Personal identification files, like passports, Social Security numbers, and birth certificates, should also be encrypted to prevent identity theft.

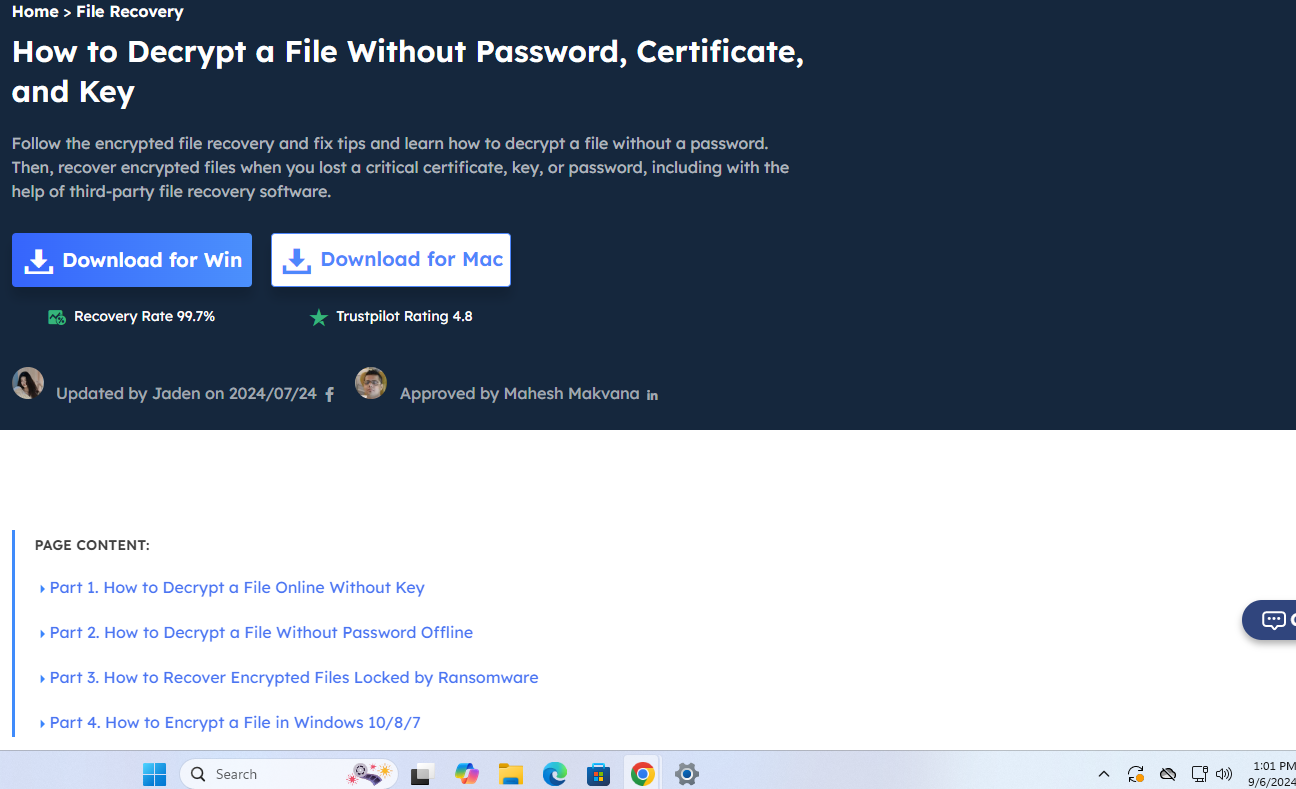
**Part2.2 (1 points)**

* 1. How to recover encrypted files without password?

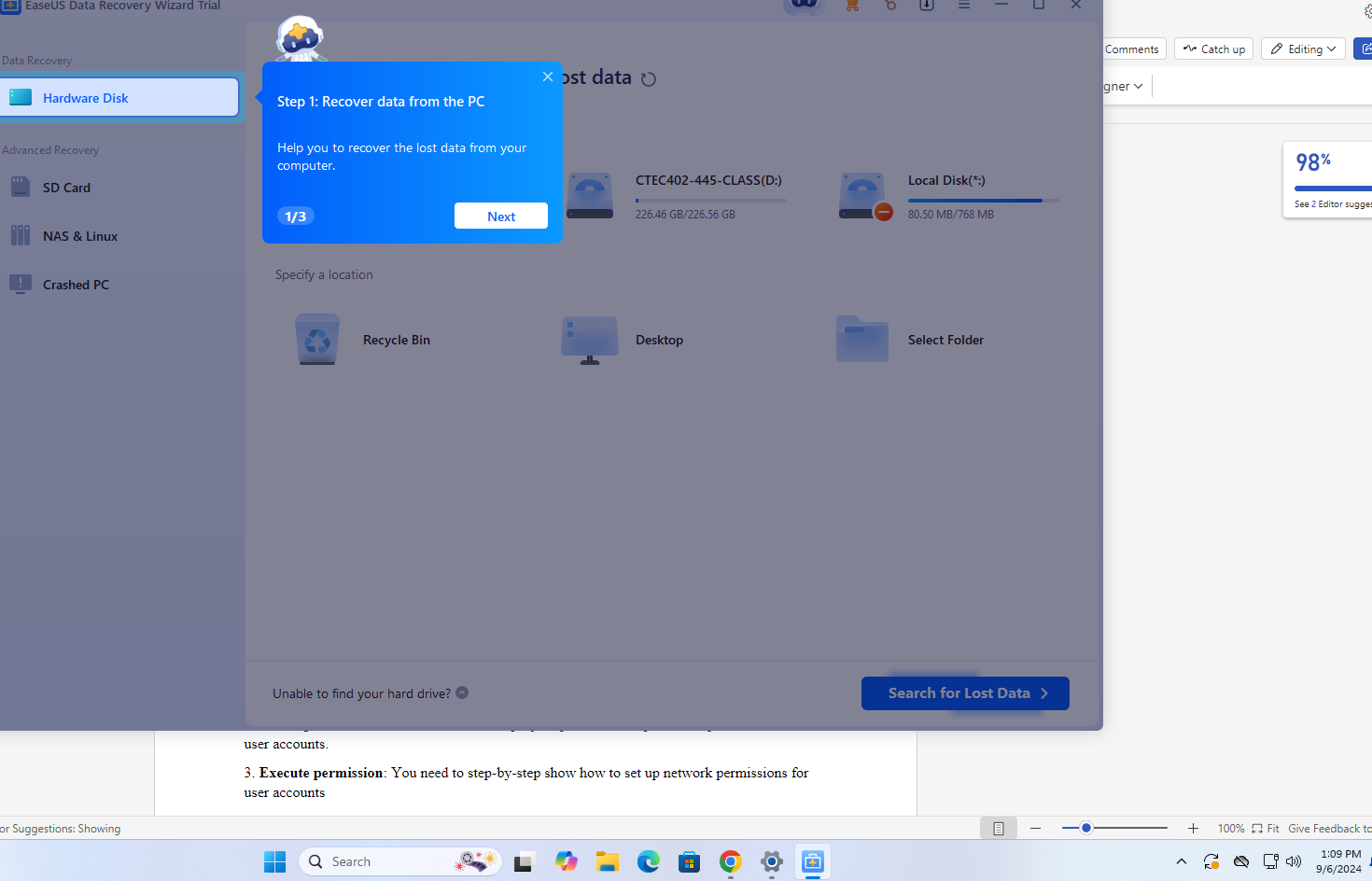
Answer: Recovering encrypted files without a password is not a simple task because once we have decided to encrypt our data, we believe no one can access the data without a password. However, if we forget our password and still want to access our data, we may try various third-party software to decrypt the data. If that option does not work, we may contact other professionals online or the company that owns the encryption technology if there is a chance that they can decrypt the cipher text.

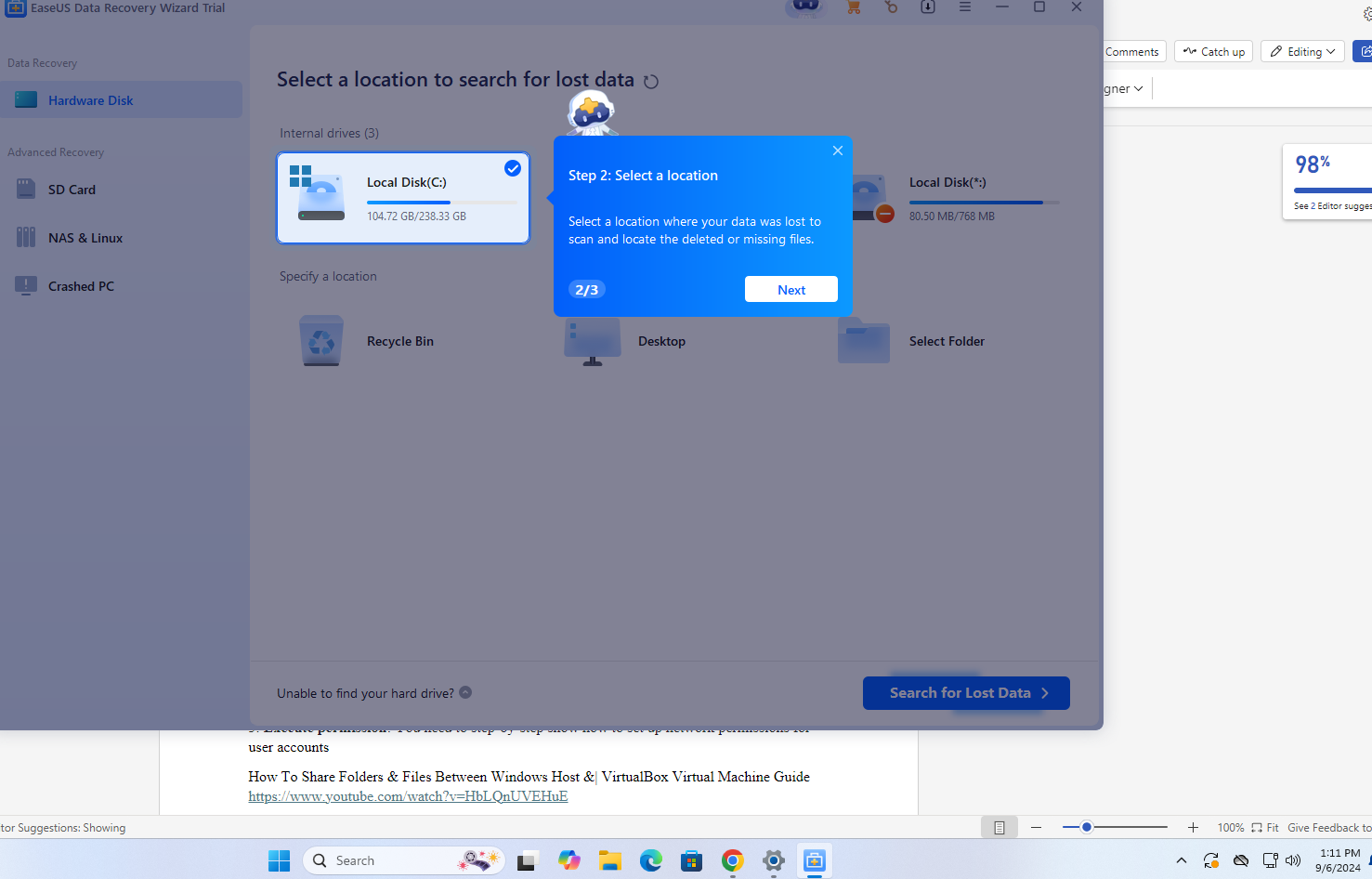
**ChatGPT**: Recovering encrypted files without a password is challenging due to the strong encryption algorithms designed to protect data. However, there are a few possible options. First, check if you have any backups of the files before they were encrypted, as restoring from a backup can bypass the need for the password. Another option is to use recovery software that attempts to crack the password through brute force or dictionary attacks, though this process can be slow and is not always successful. For highly valuable data, professional recovery services might offer advanced tools to handle more complex encryption scenarios.

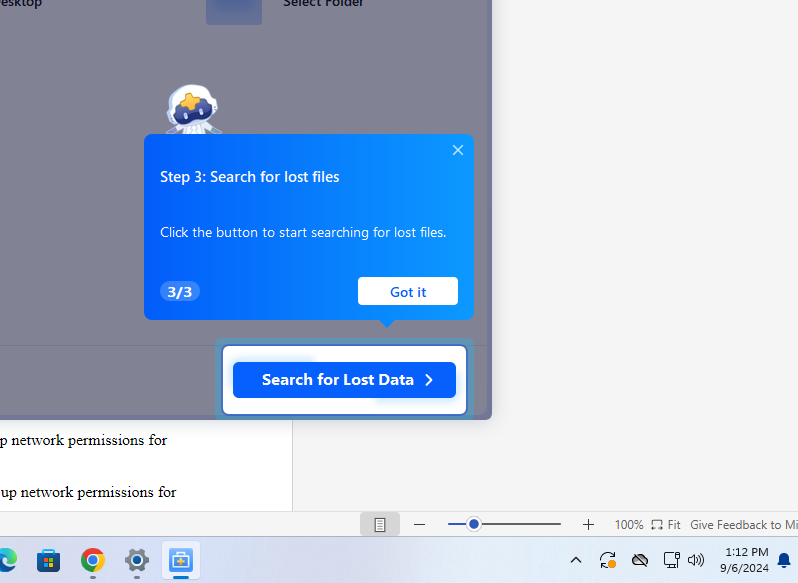
You need to download a free tool which shows how to recover your encryption key and make sure to create step-by-step documentation. <https://www.easeus.com/file-recovery/recover-encrypted-files-without-certificate.html>

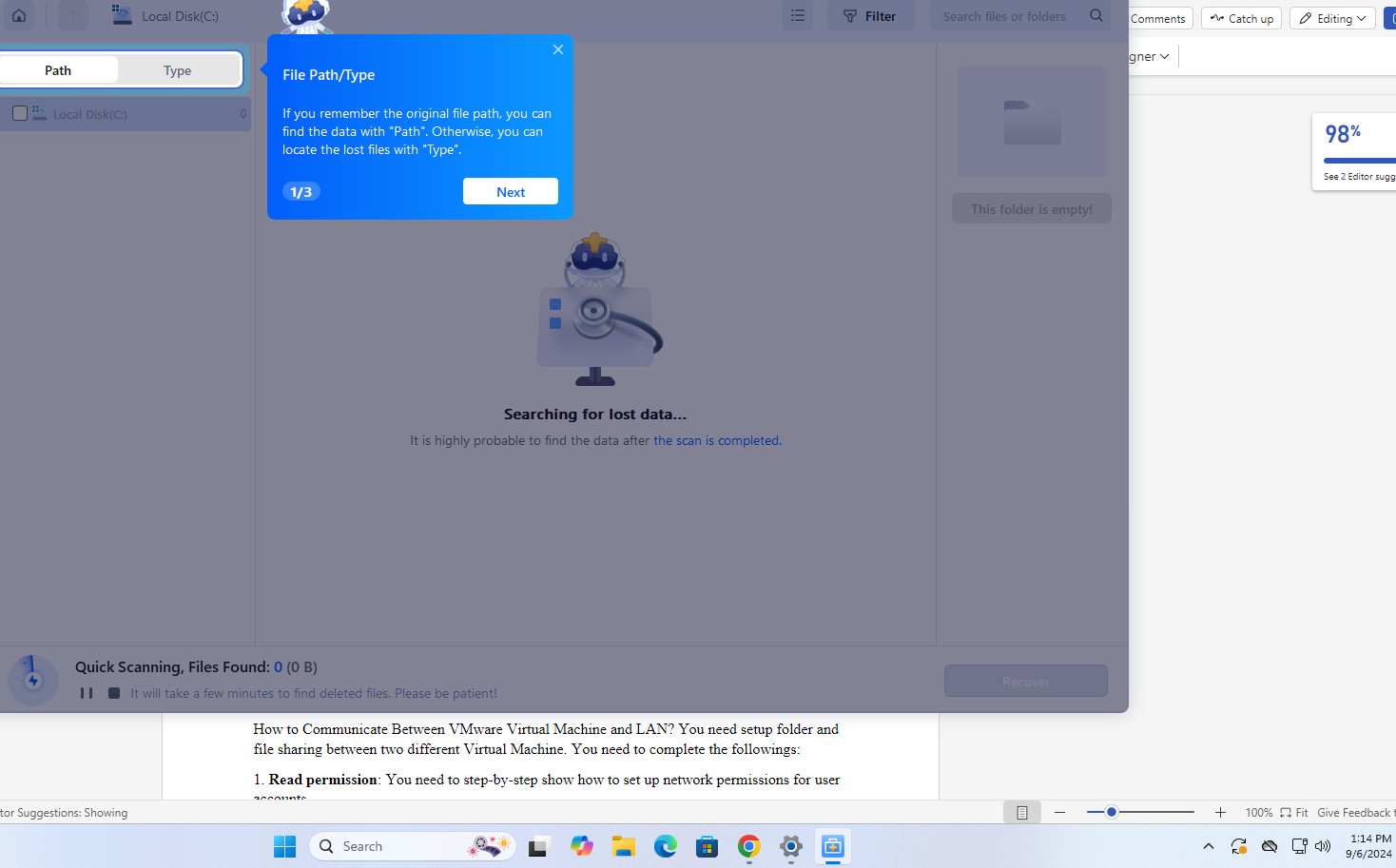
**Step 1. Go To the** **Easeus.Com Official Website and Download the Encrypted File Recovery File** 

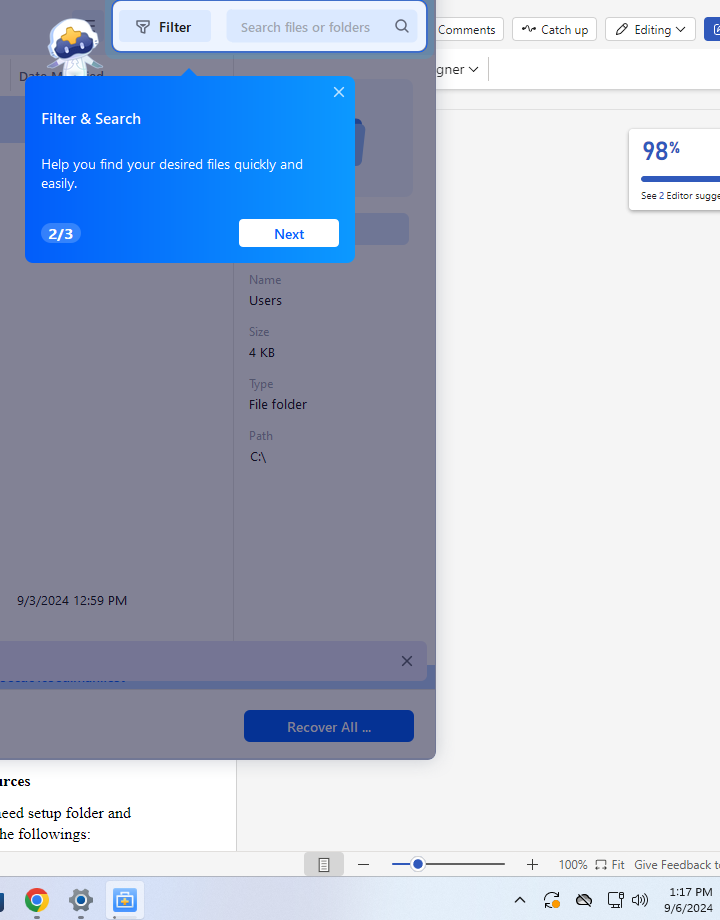
**Step 2: Click The Download for Win Button and Run It** 

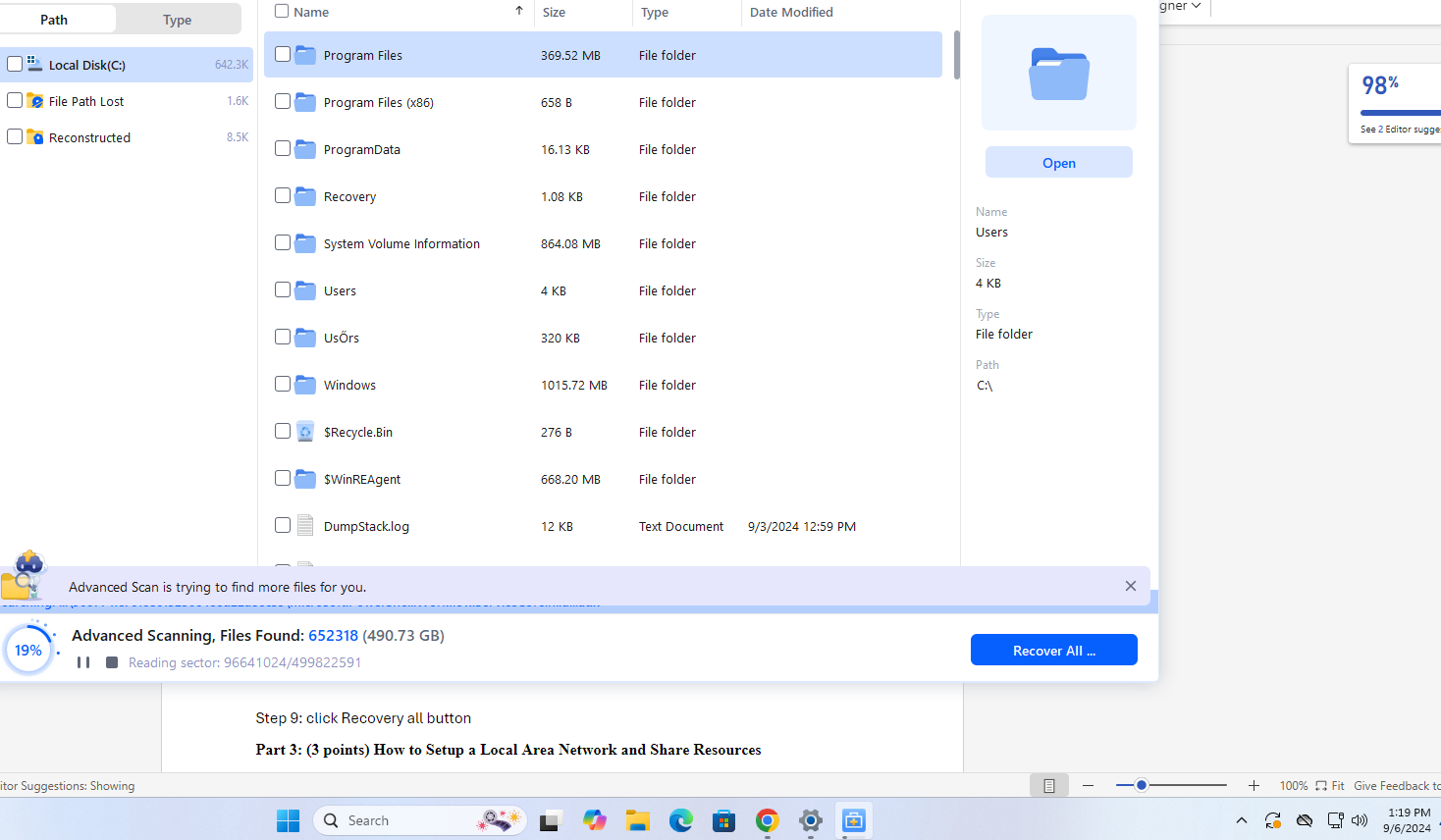
Step 3: click the install button and continue the process

Step 4: click next to select location 

**Step 5: click search for lost data button** 

**Step 6: click next to find the search path** 

**Step 7: Click filter to customs our selection** 

**Step 9: click Recovery all button** 

**Part 3: (3 points) How to Setup a Local Area Network and Share Resources**

How to Communicate Between VMware Virtual Machine and LAN? You need setup folder and file sharing between two different Virtual Machine. You need to complete the followings:

1. **Read permission**: You need to step-by-step show how to set up network permissions for user accounts.

2. **Write permission:** You need to show step-by-step how to set up network permissions for user accounts.

3. **Execute permission**: You need to step-by-step show how to set up network permissions for user accounts

How To Share Folders & Files Between Windows Host &| VirtualBox Virtual Machine Guide <https://www.youtube.com/watch?v=HbLQnUVEHuE>

YouTube video show: Windows 11- How to Share Files, Folders & Drives Between Computers Over a Network <https://www.youtube.com/watch?v=X5aqtAtBB6w>

**Part 4: video**