Module 20 Cryptography

1 what is cryptography

2 types of encryption

- Symentric encryption
- Asymentric encryption

Task1 how to encryption and decryption file and folder in windows

3 What is digital signature

4🔧 How a digital signature works

MAYUR

Task2 how to Confidential Data Encryption with VeraCrypt on Windows

MAYUR

1 what is cryptography

Cryptography is the practice and study of techniques for **securing communication and data** in the presence of adversaries. It ensures that information is **kept confidential**, **unmodified**, and **authentic** when being stored or transmitted.

📖 **Definition**:
Cryptography is the science of converting **plaintext** into **ciphertext** using mathematical algorithms to protect it from unauthorized access.

🔄 **Cryptography Process:**

Cryptography follows a well-defined **process** to convert readable data (plaintext) into an unreadable format (ciphertext) and then back to readable format using encryption and decryption

2 types of encryption

Encryption is a fundamental aspect of data security, transforming readable information into an unreadable format to prevent unauthorized access. There are several types of encryption, each with its unique characteristics and use cases

🔐 **Symmetric Encryption**

MAYUR

Symmetric encryption uses the same key for both encryption and decryption. It's efficient and commonly used for encrypting large volumes of data. However, secure key distribution is a challenge.

- **Examples**: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish, and Twofish.

🔑 Asymmetric Encryption

Also known as public-key cryptography, asymmetric encryption employs a pair of keys: a public key for encryption and a private key for decryption. This method enhances security, especially in digital communications

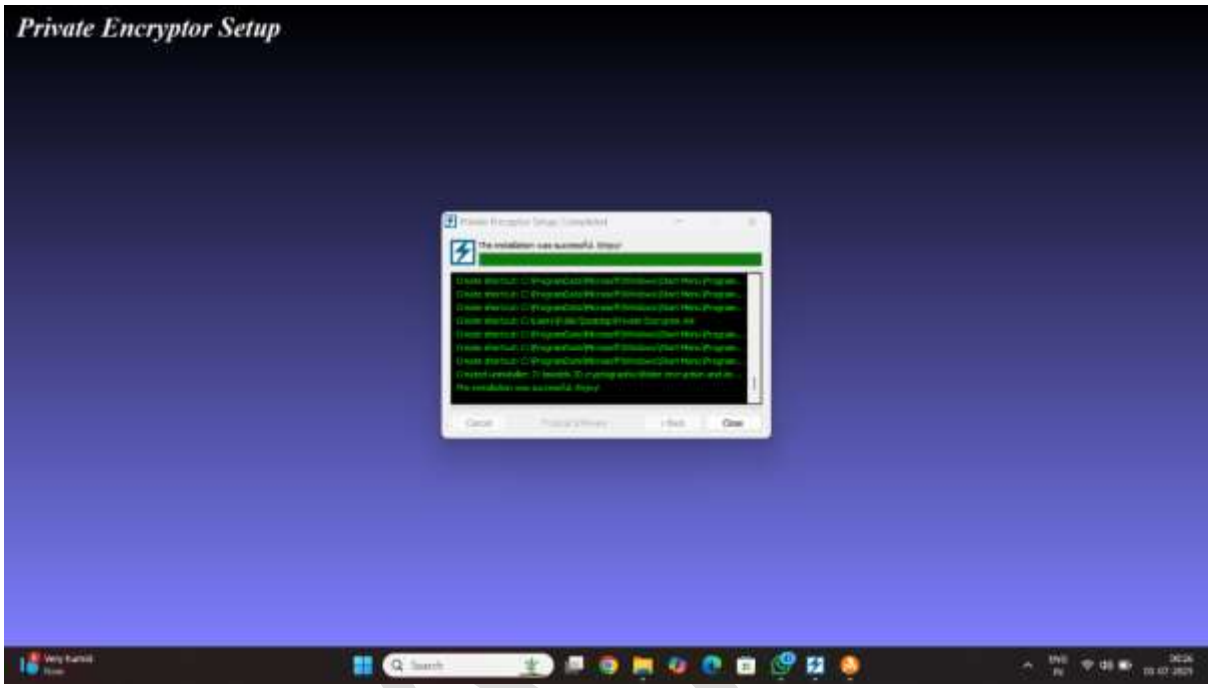
Examples: RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman.

MAYUR

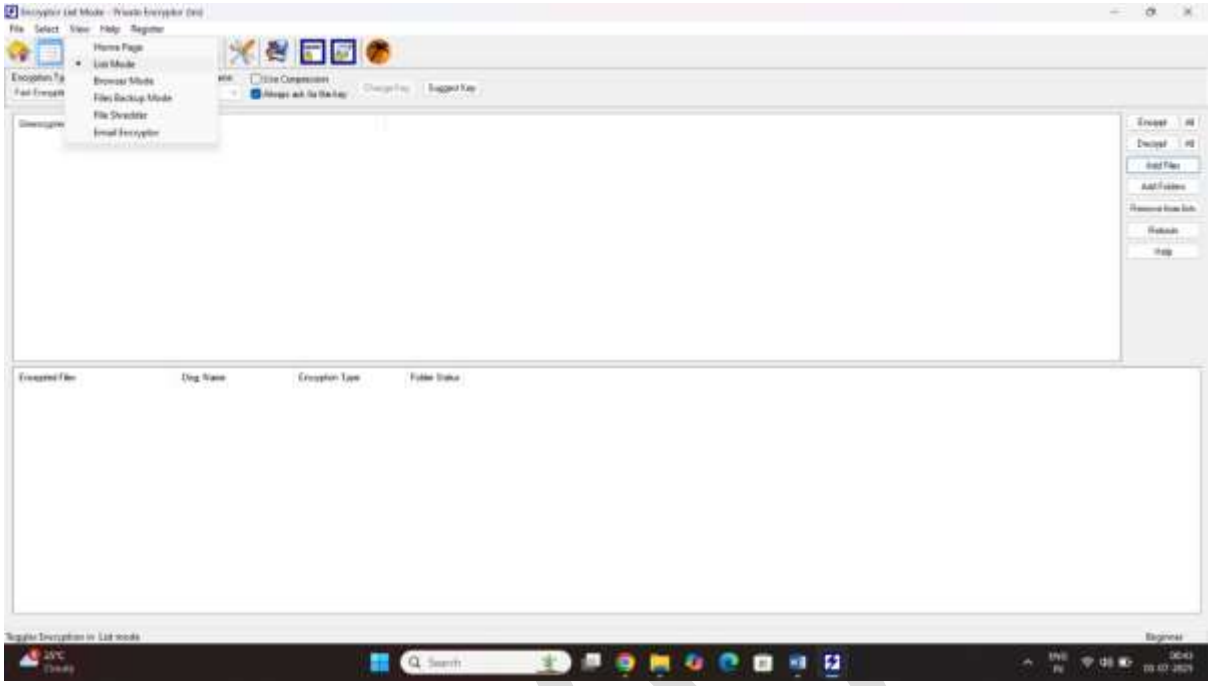
Task1 how to encryption and decryption file and folder in windows

Step1 download the encryptorsetup

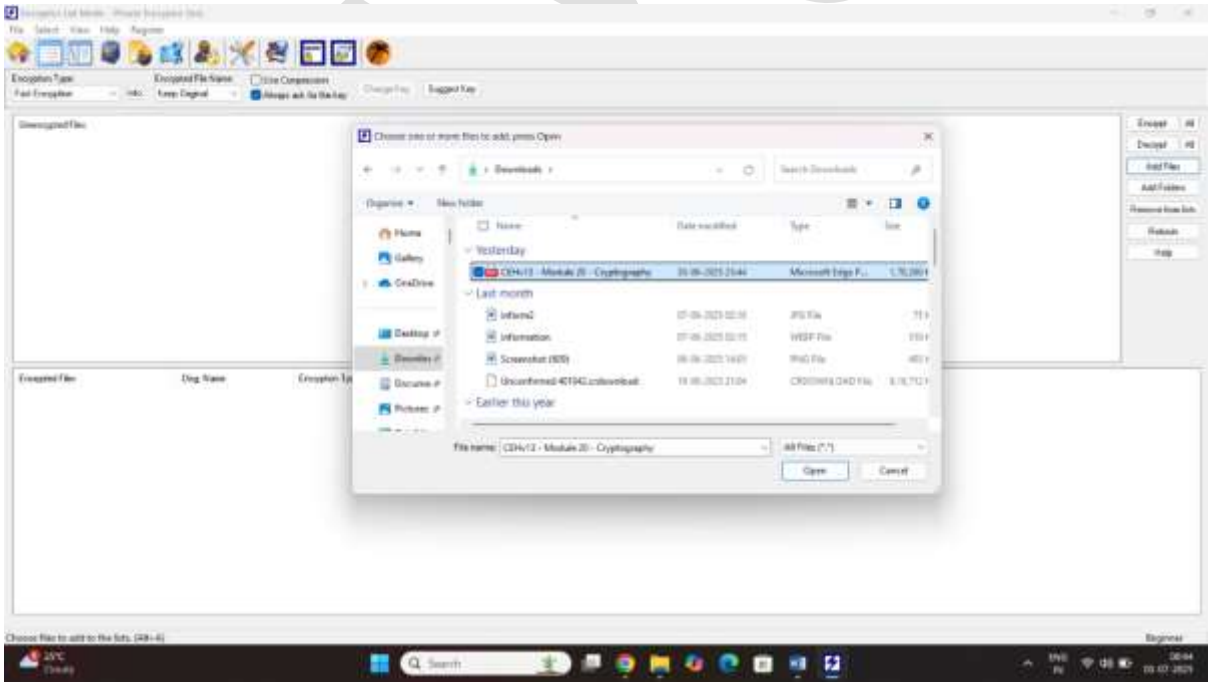
Step 2 start the encryptor setup in windows



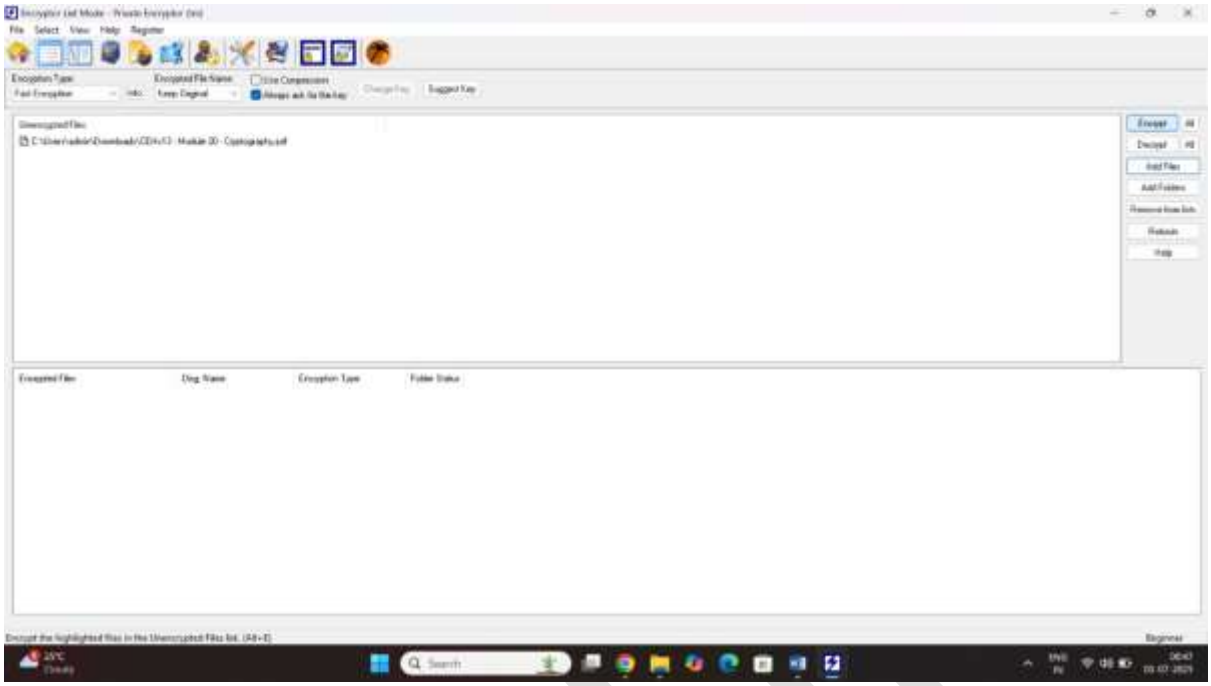
Step3 Select the list mode



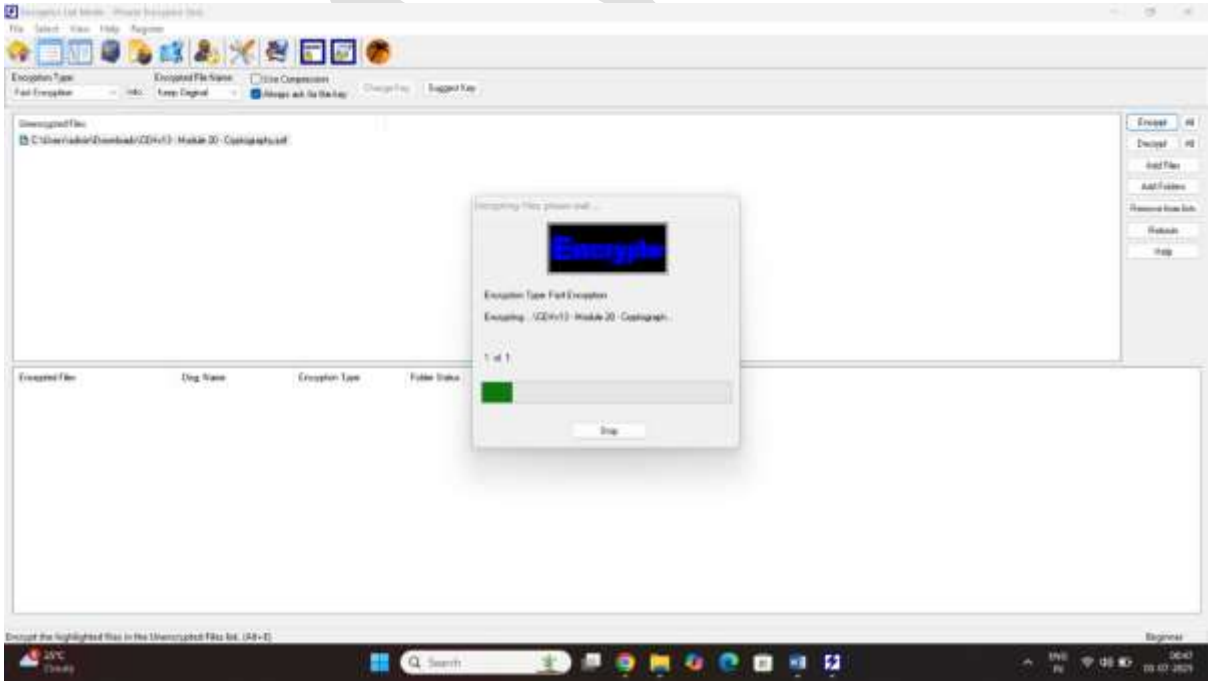
Step4 click on the add file



Step5 select the encrypt option

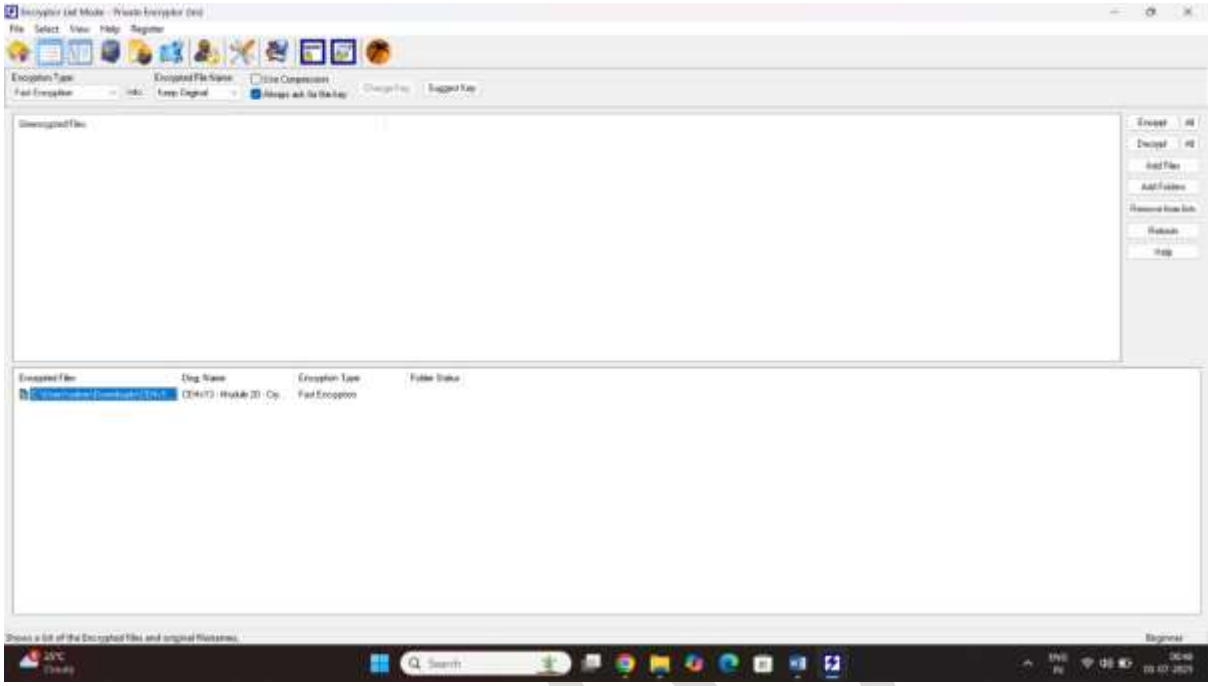


Step6 click on the encrypt option

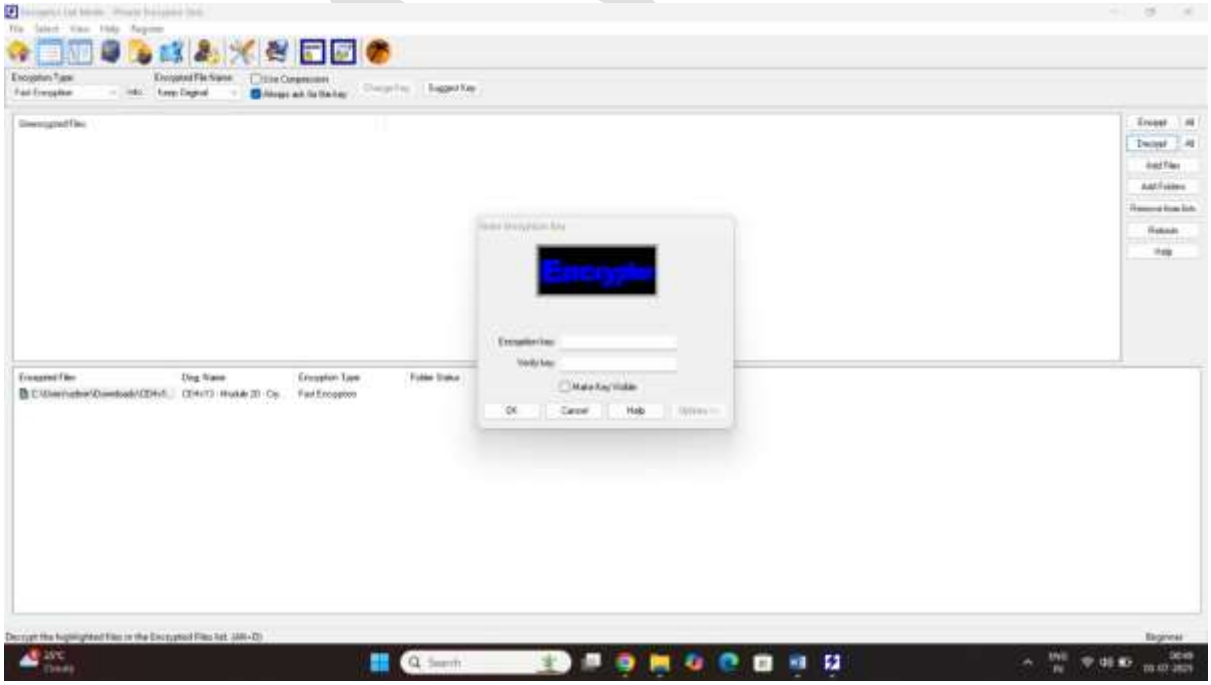


Decryption method

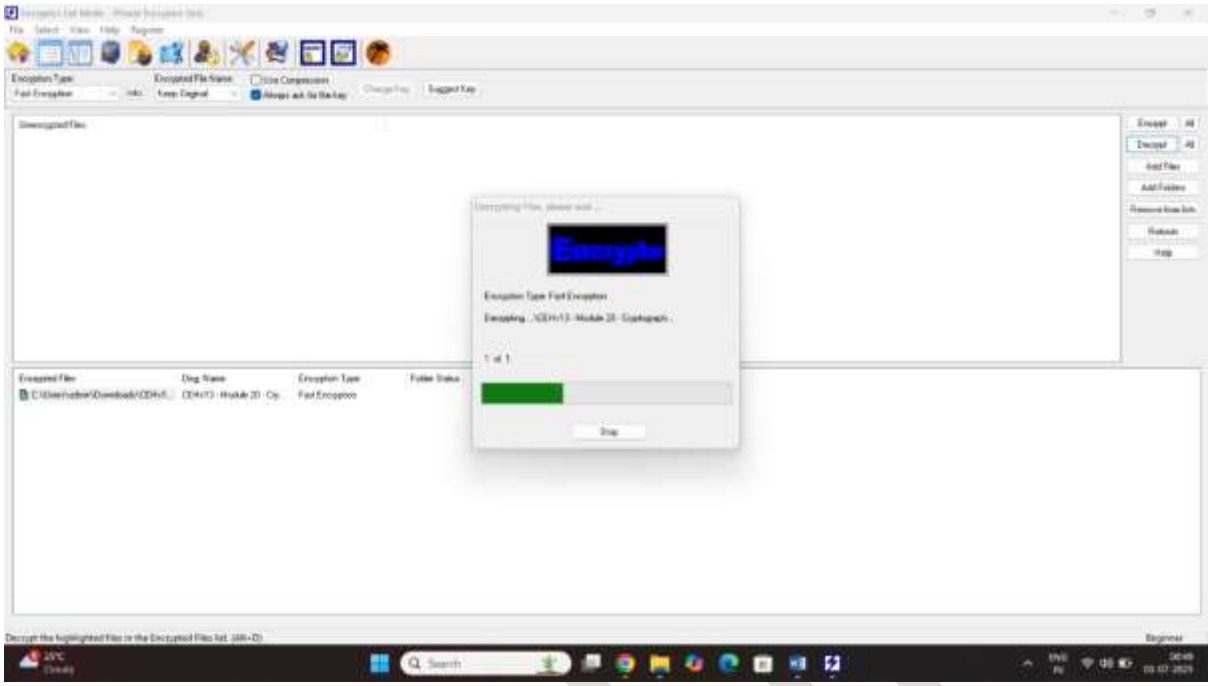
Step1 select the decryption file

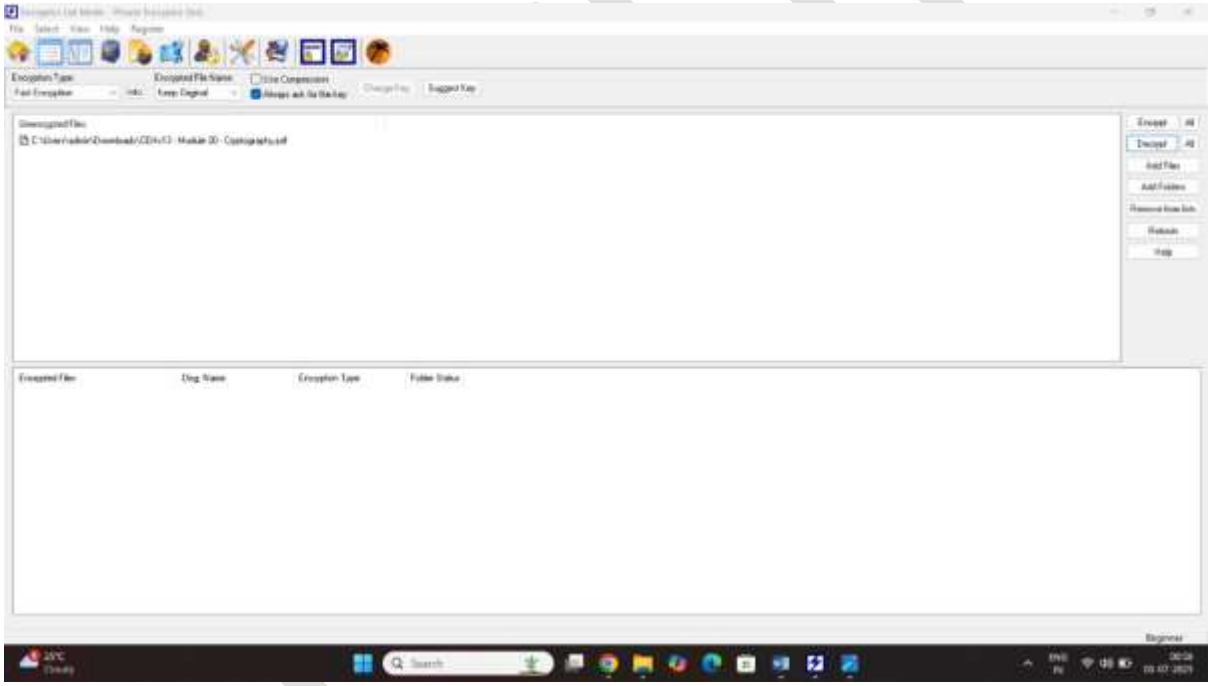


Step2: click on decryption option



Step3 enter the encryption password





What is digital signature

A **digital signature** is a cryptographic method using asymmetric encryption (a private key for signing and a public key for verification) to ensure that a digital document truly comes from the claimed sender and hasn't been altered It works by hashing the document, encrypting that hash with the signer's private key, and sending both the document and encrypted hash together . The recipient decrypts the hash with the public key and compares it to their own hash of the document—matching hashes prove authenticity and integrity

Beyond verifying origin and integrity, digital signatures provide **non-repudiation**, meaning the signer cannot later deny having signed the document, since only their private key could have produced that signature They commonly rely on **certificate authorities and PKI** to issue digital certificates that tie public keys to specific identities, making them legally valid in many countries This makes digital signatures widely used in secure contracts, software distribution, e-filing, and financial transactions.

MAYUR

🔧 How a digital signature works

- A **hash** (a fixed-length digital fingerprint) of the document is computed.
- This hash is **encrypted with the signer's private key**, forming the digital signature.
- Both the document and signature are sent to the recipient.
- The recipient **decrypts the signature** using the signer's **public key** and computes a new hash of the document.
- If the two hashes match, the signature is **valid**—confirming sender identity and that the document is unmodified

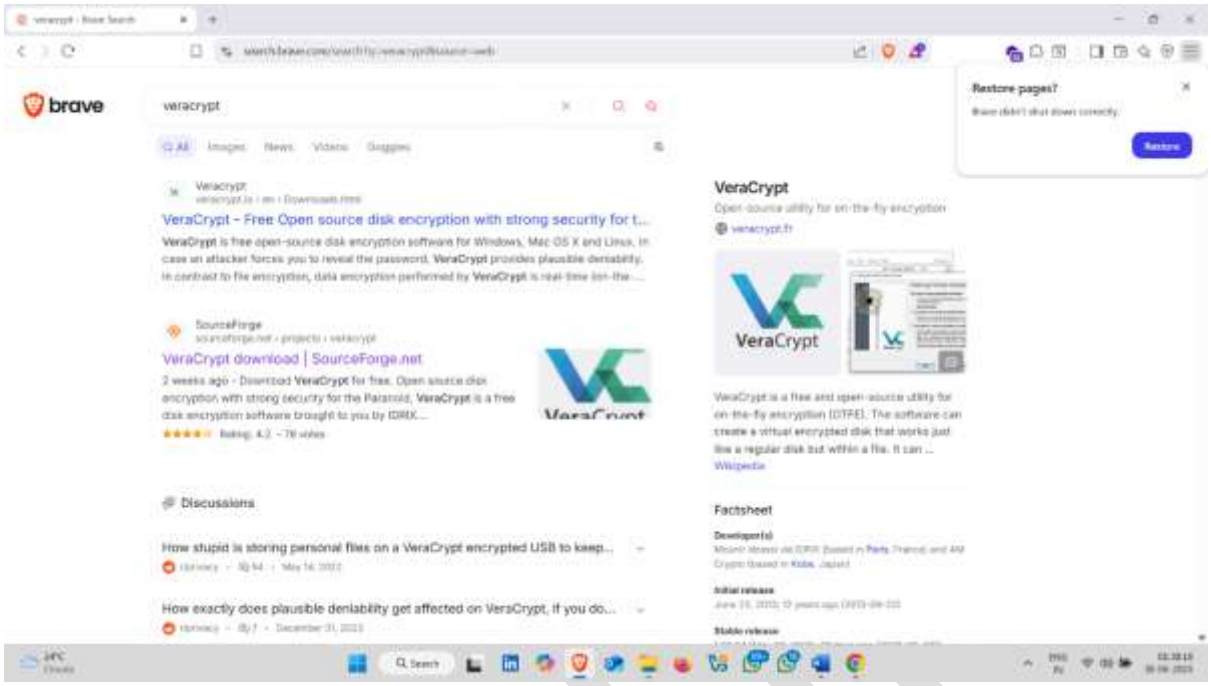
MAYUR

Task2 how to Confidential Data Encryption with VeraCrypt on Windows

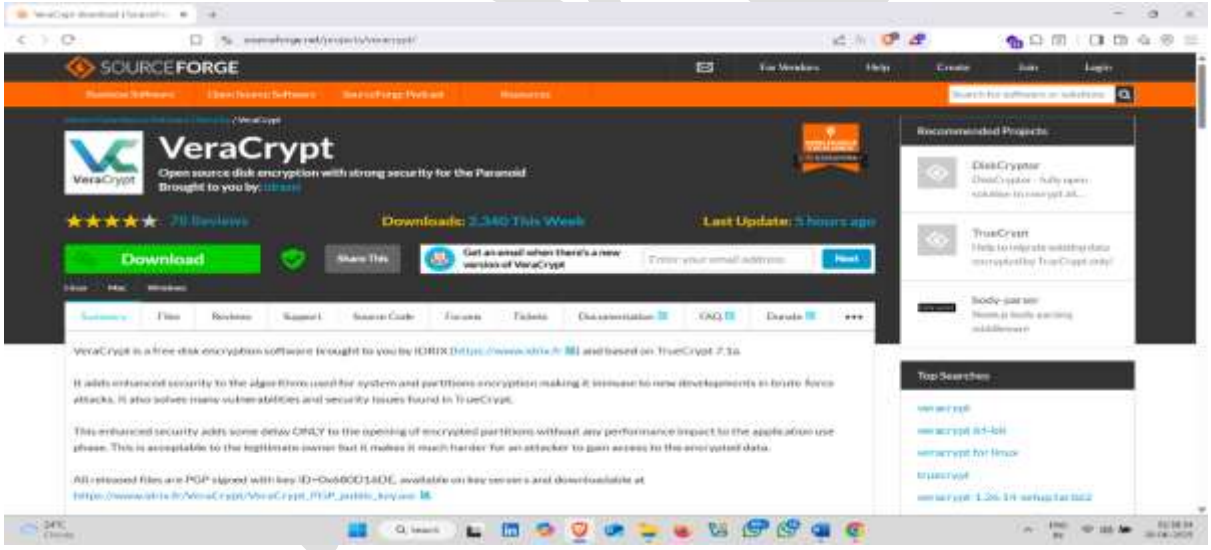
How to download it -:

Step1 Open Browser and search **Veracrypt**

Step2 Click on second website – **Source Forge**



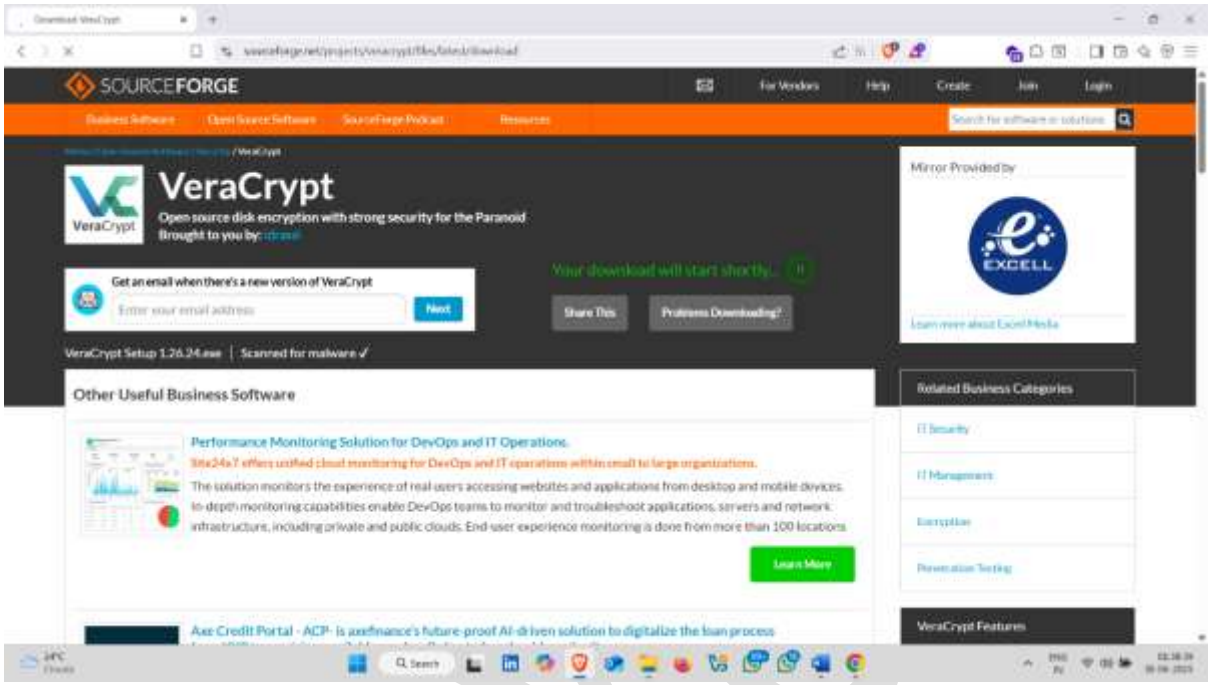
Step3 click on Download



Step4 Download Started automatically

Download Link-:

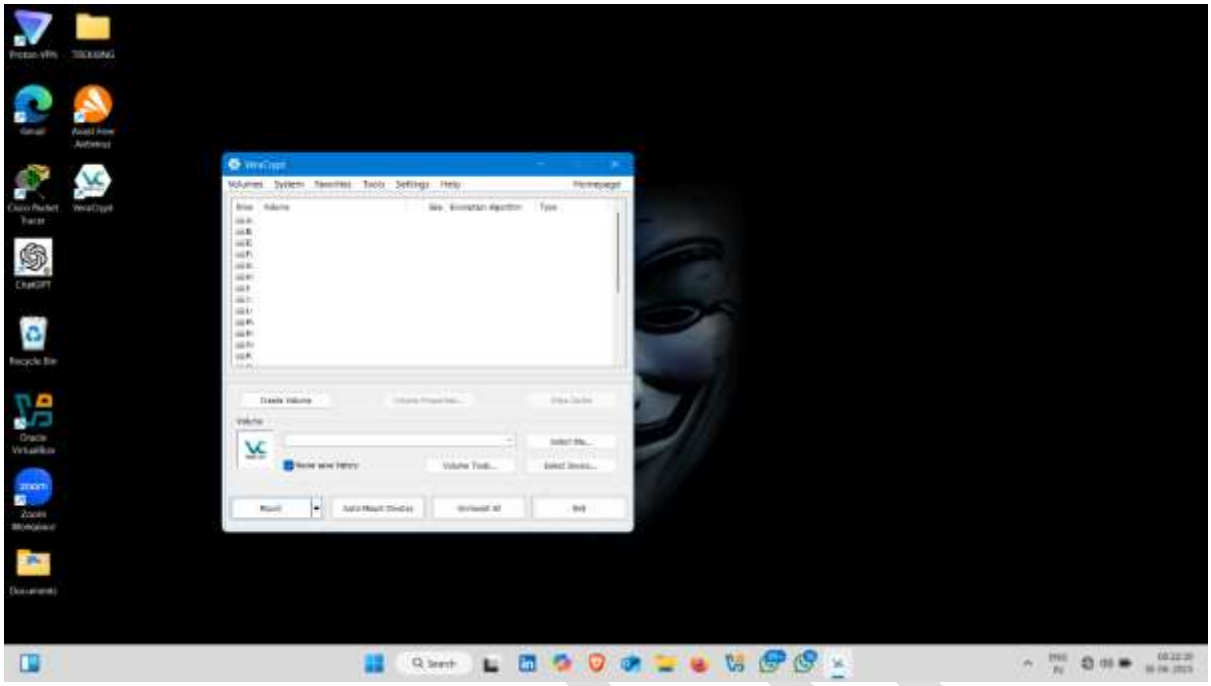
https://sourceforge.net/projects/veracrypt/



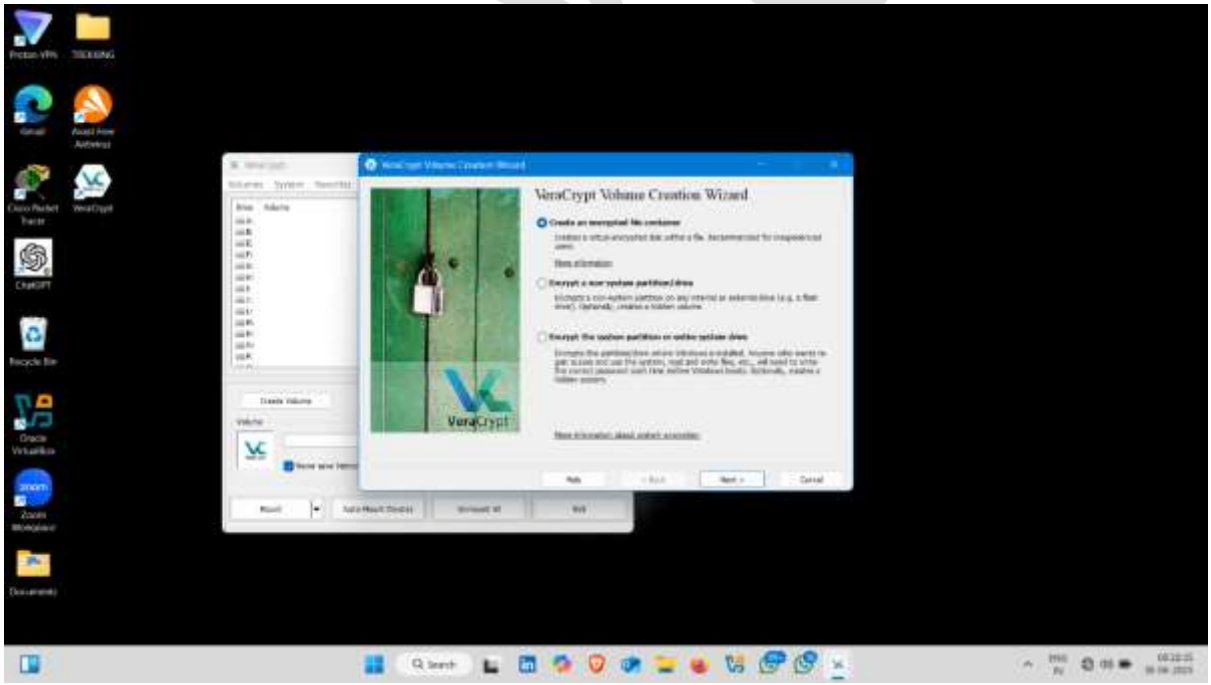
How to use it -:

Step1 After setup **veracrypt** open it

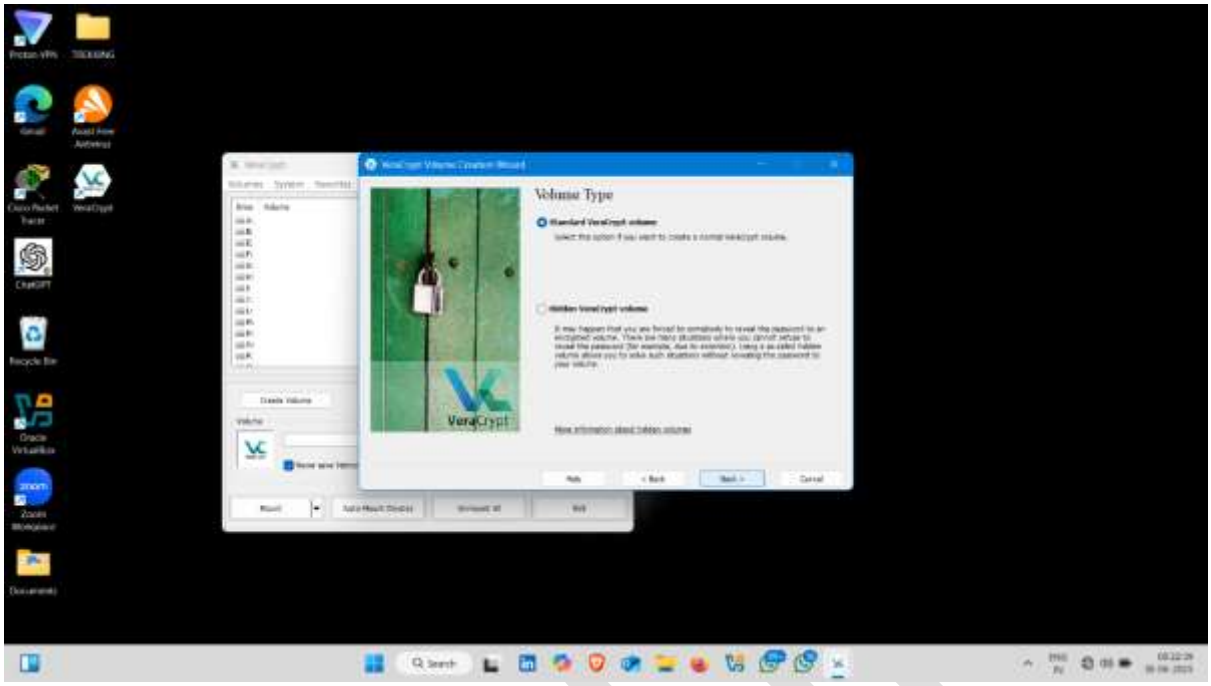
Step2 Click on **create volume**



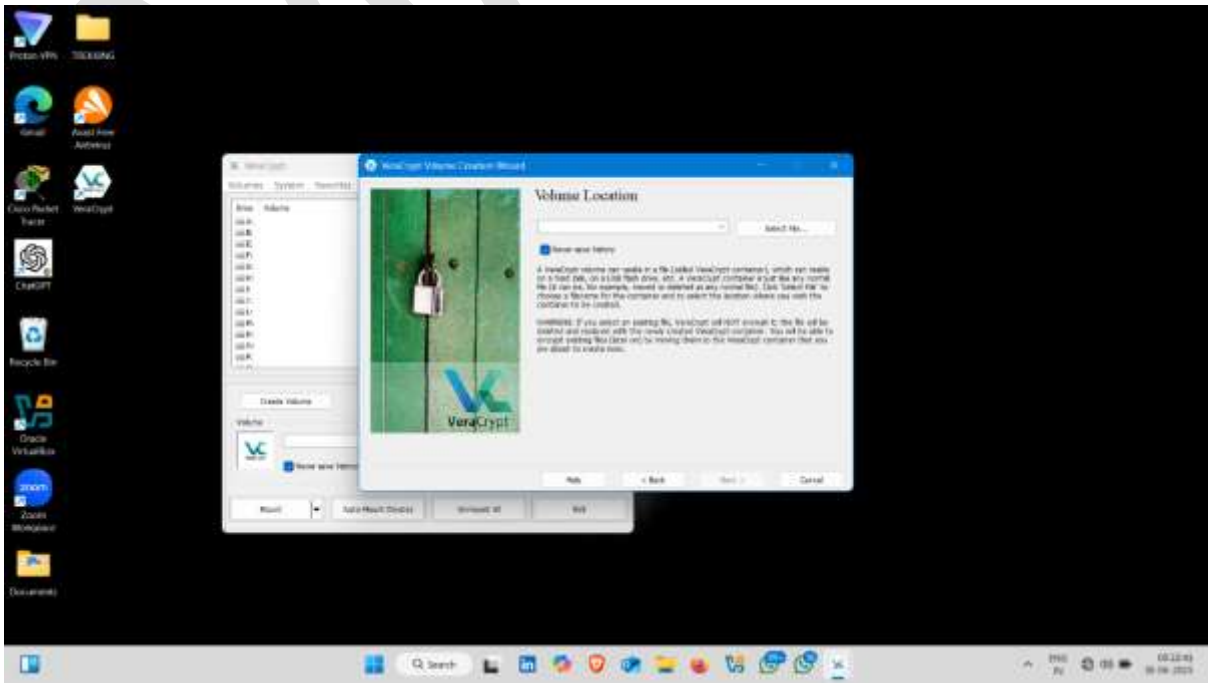
Step3 Select first option – **Create an encrypted file container**



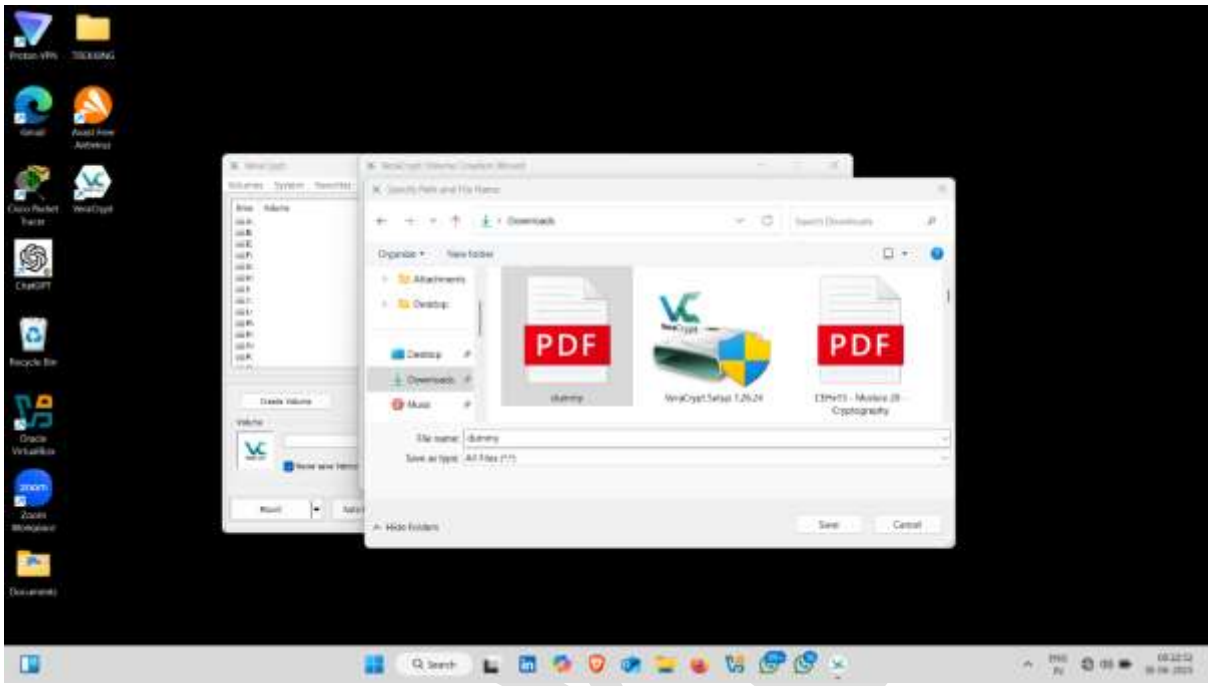
Step4 Now select first option – **Standard VeraCrypt volume**



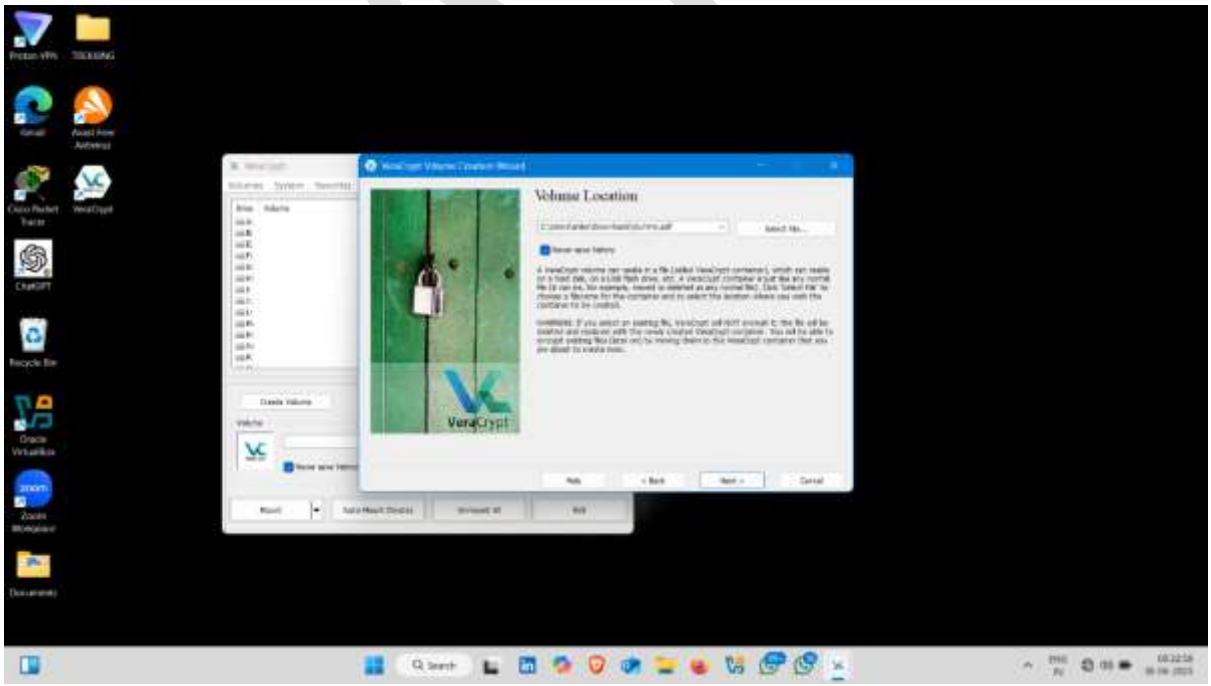
Step5 Select file that you want to encrypted



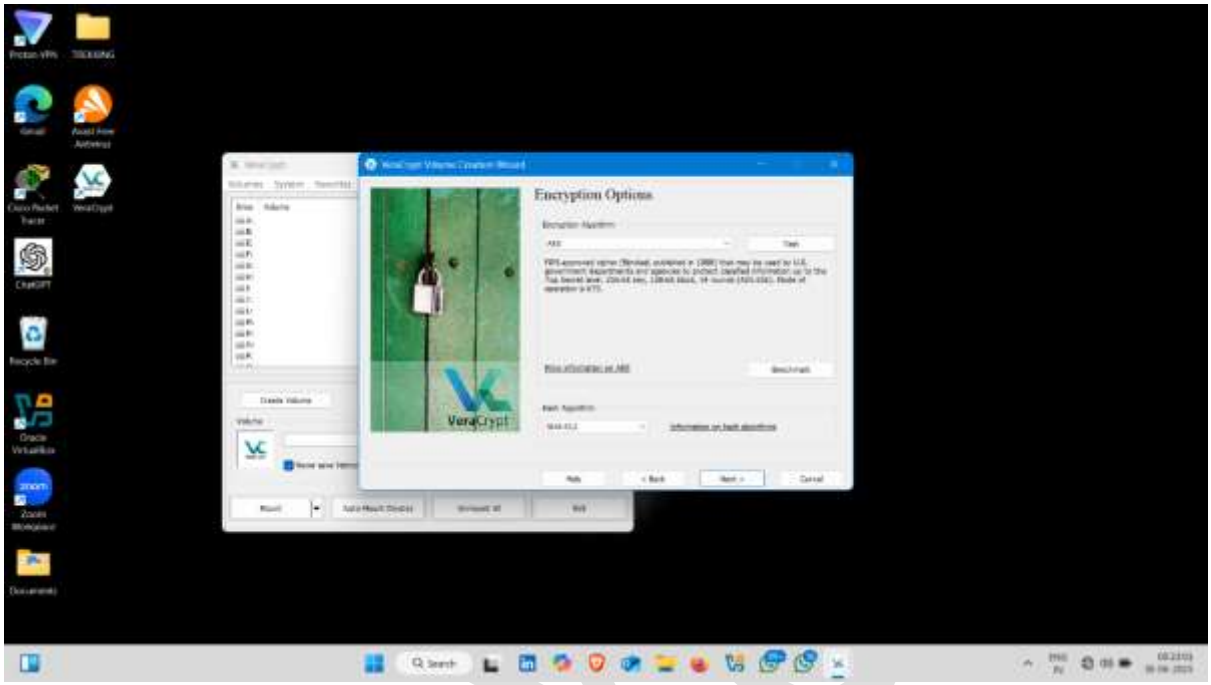
Click on **save**



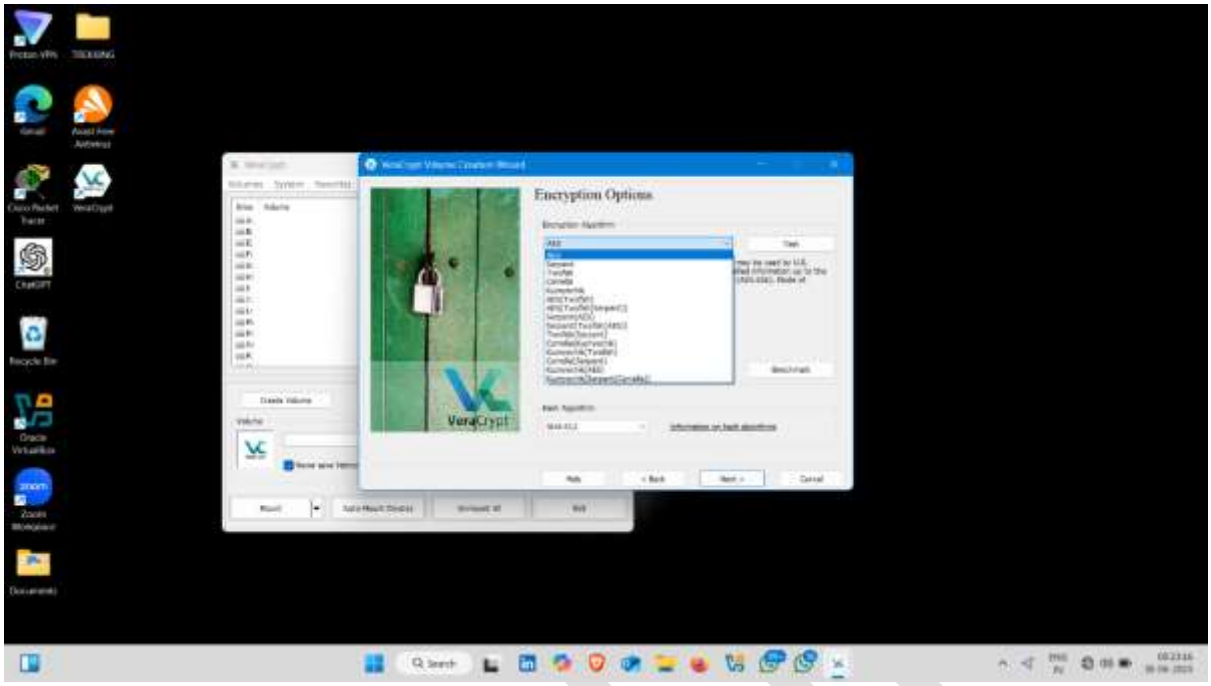
Step6 Click on next



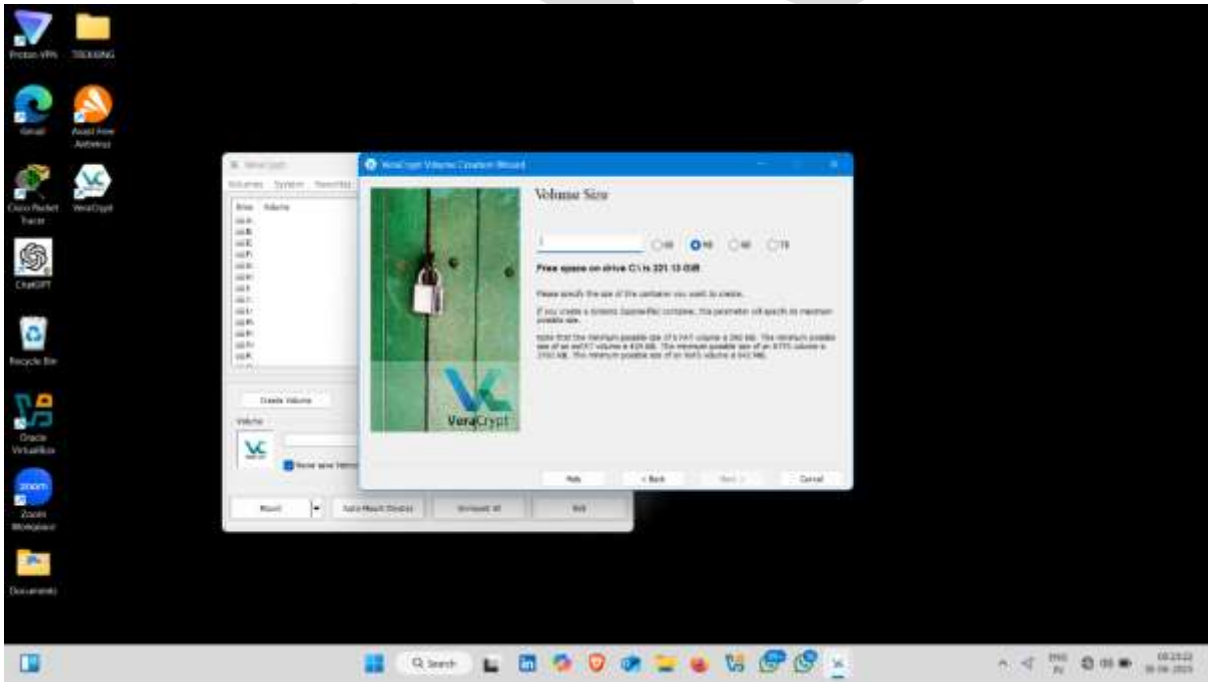
Step7 Click on drop-down arrow ▼ – to select encryption type



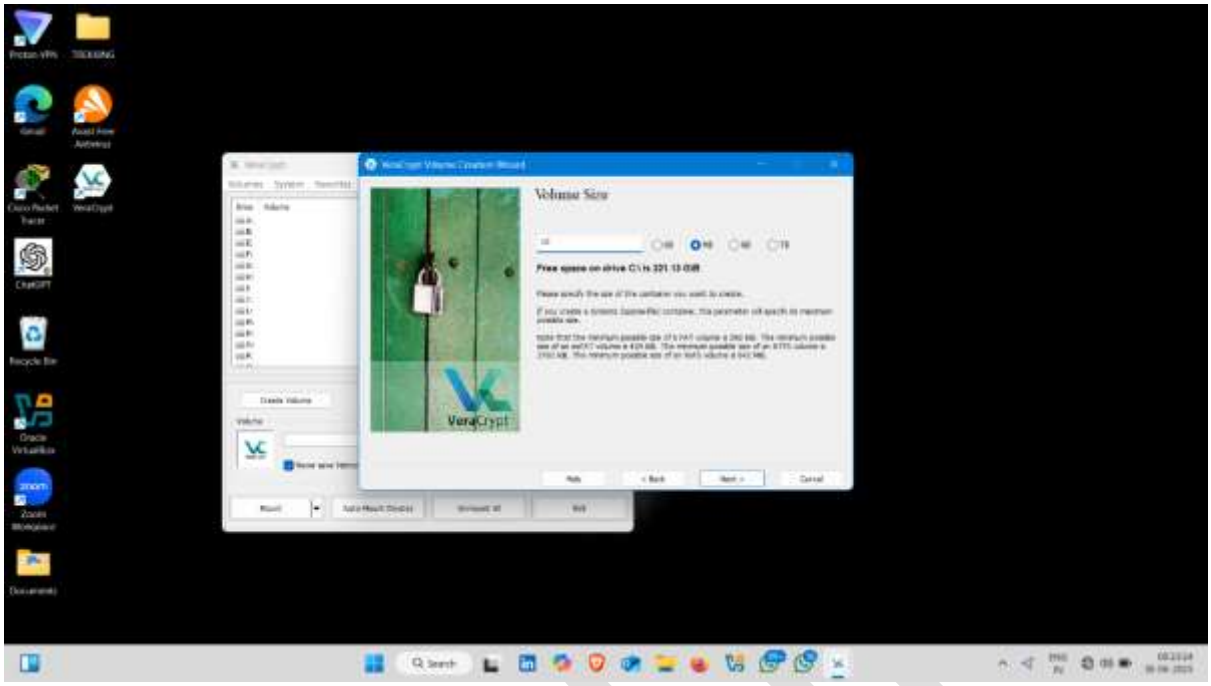
Step8 Click on **next**



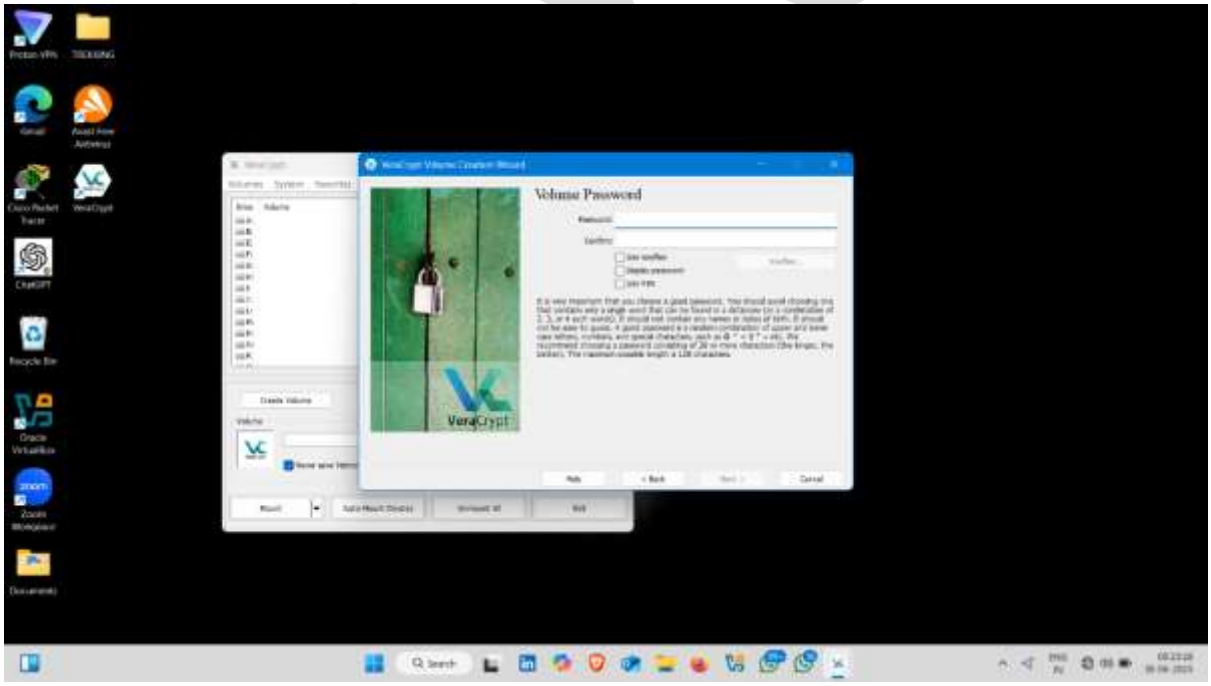
Step9 Select **free space on drive**



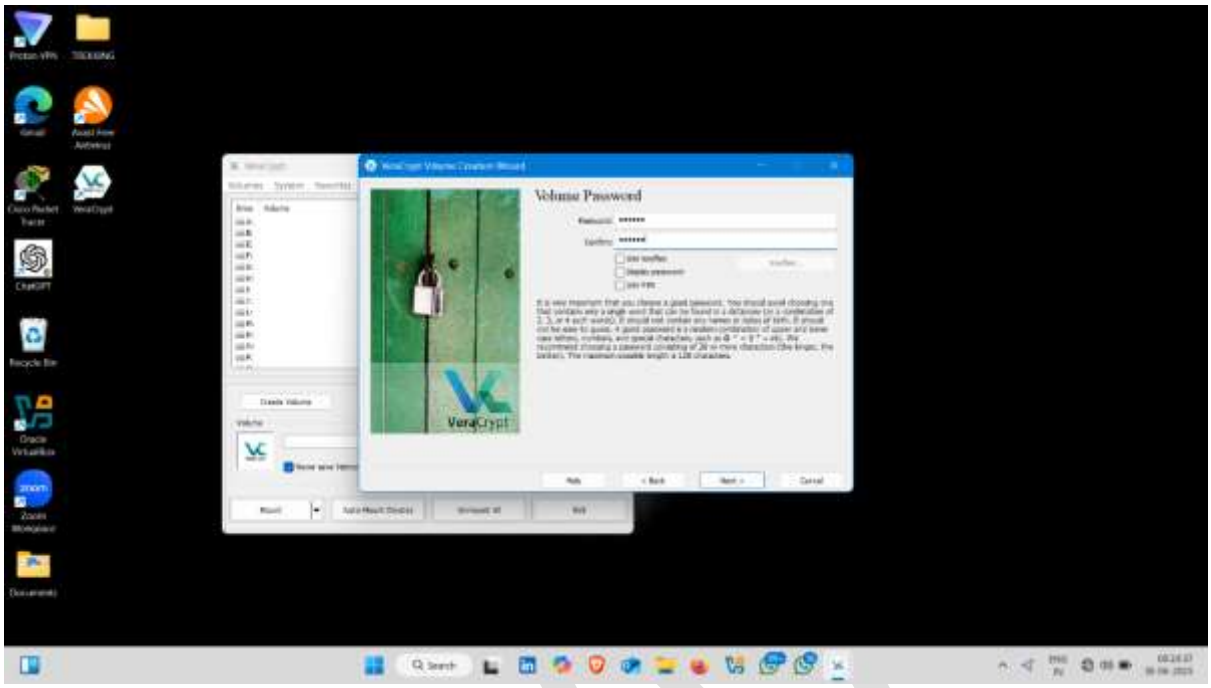
Step 10 Click on **next**



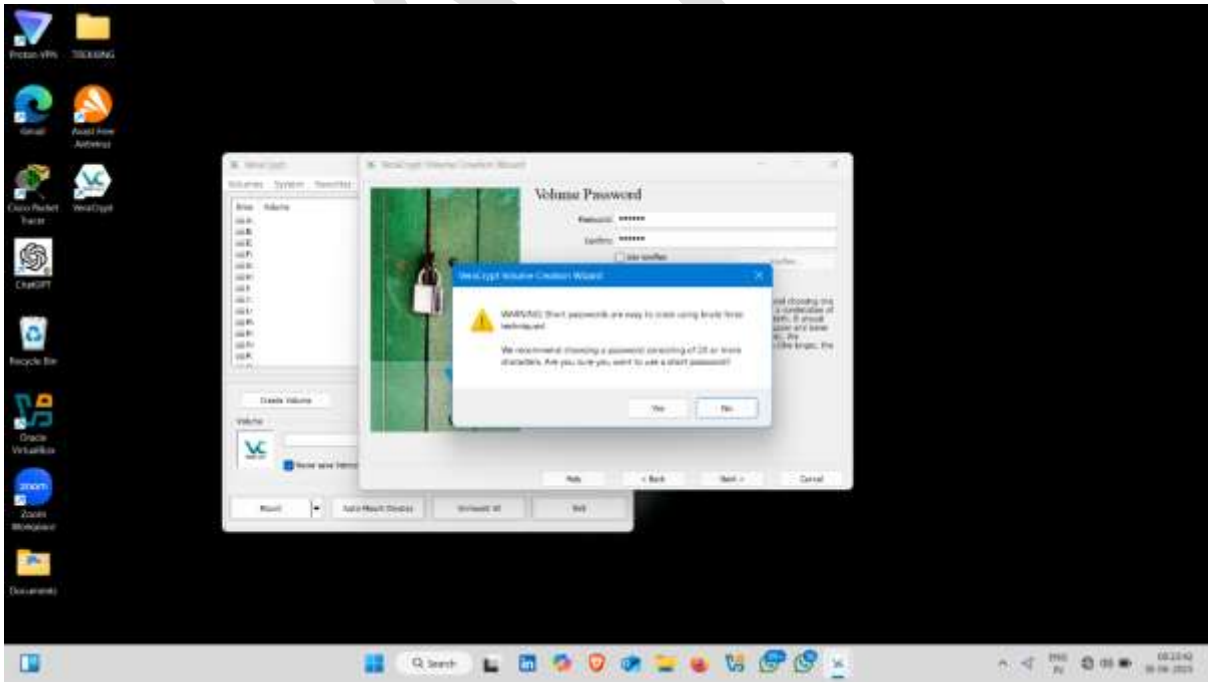
Step11 now set a **password**



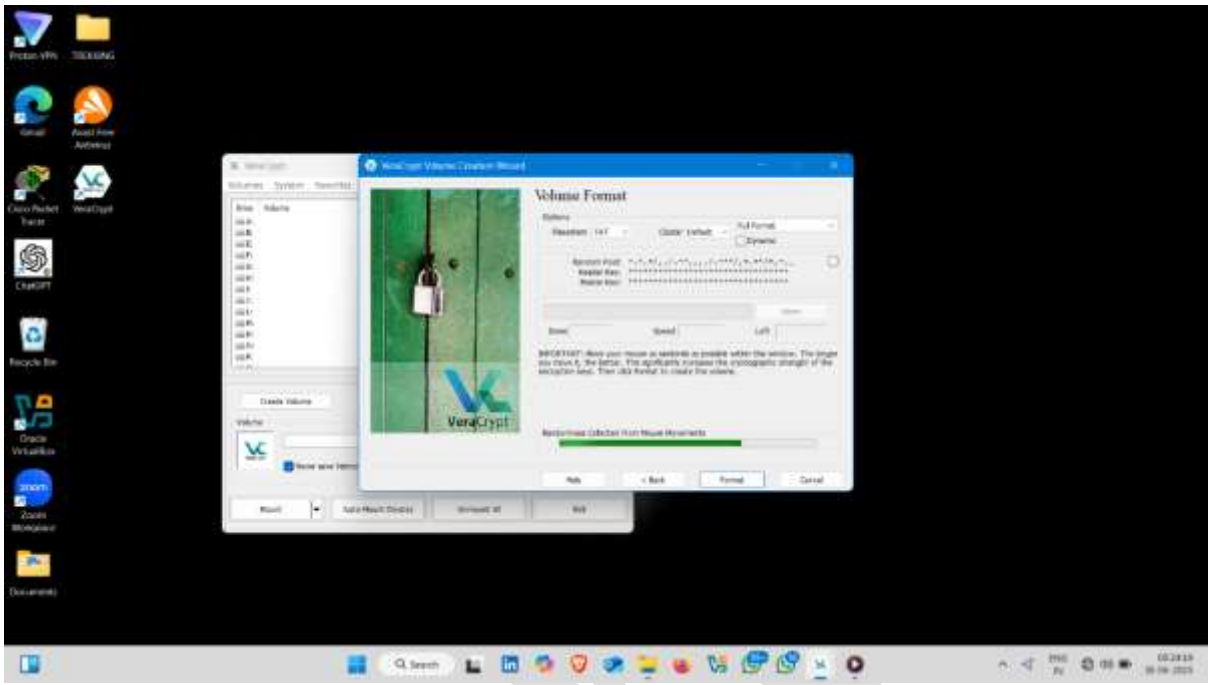
Step12 click on **next**



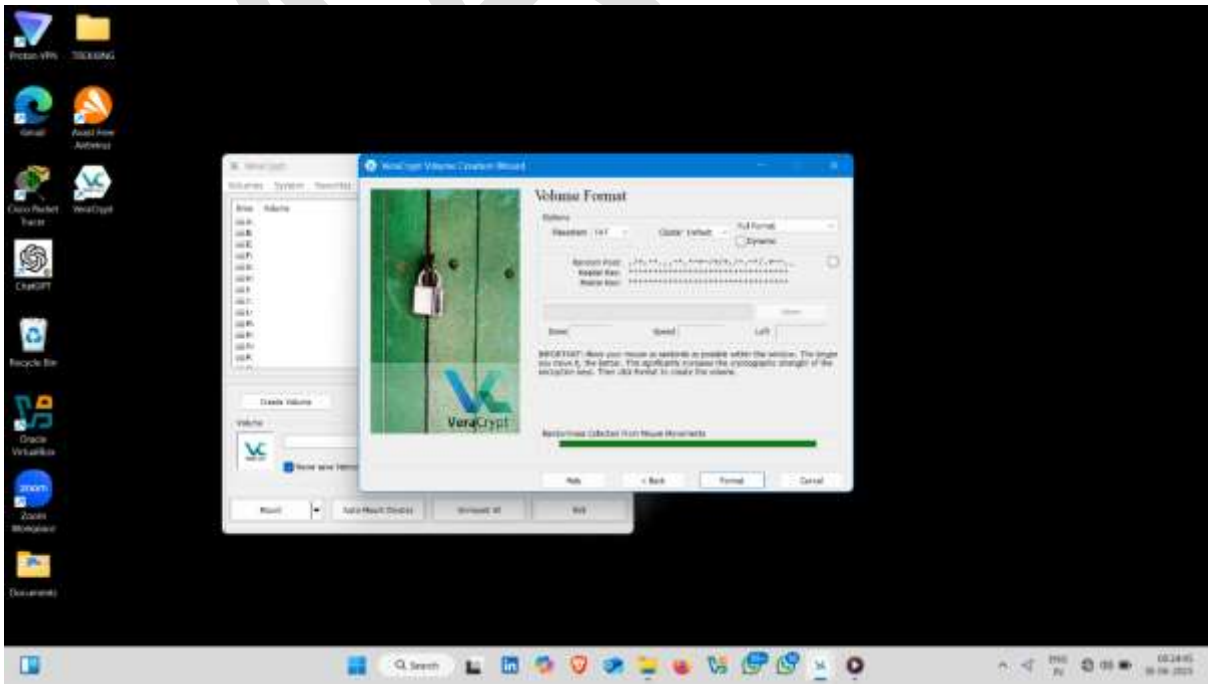
Step 13 click on **yes** ✓



Step 14 Encryption started ✓👇



Step 15 Click on **format**



MAYUR