
VeraCrypt

What is VeraCrypt

VeraCrypt သည် မိမိရဲ့ Computer ထဲမှာရှိတဲ့ အရေးကြီး Data အချက်အလက်တွေ သိမ်းဆည်းရန် အတွက် လုံခြုံရေး အားကောင်းပြီး ချိုးဖျက်ရ မလွယ်ကူသော Data Encryption Software ဖြစ်ပါသည်။

Veracrypt တွင် မိမိ၏ အရေးကြီးသော အချက်အလက်များကို အခန်းများ (Folder များ) ခွဲကာထည့်၍ အခြားလူများ သတိမထားမိအောင် ပုံစံပြောင်းပြီး လုံခြုံတဲ့ Password များပေးကာ သိမ်းဆည်းထားနိုင်ပါသည်။

Veracrypt သည် File folder အသစ်များကို တည်ဆောက်ထားလို့ရသလို မိမိရဲ့ Computer ထဲမှ Drive Folder များကိုလဲ အခန်းခွဲ၍သော့ခတ်နိုင်ပါသည်။ ထို့အပြင် Hard Disk , Memory Stick များကိုလဲ Veracrypt ကိုအသုံးပြု၍ Password ထားကာ အခန်းများခွဲ၍ လုံခြုံအောင်ပြုလုပ်နိုင်ပါသည်။

VeraCrypt ကို ကွန်ပျူတာတွေထဲတွင်သာ ထည့်သွင်းအသုံးပြုနိုင်ပါသည်။

What is VeraCrypt

Veracrypt ကို Download ဆွဲရန်အတွက် ကိုယ့် Computer မှ Browser တစ်ခုခုကိုဝင်ပါ။ Veracrypt လို့ ရိုက်ရှာပါ ။
https://www.veracrypt.fr/code/VeraCrypt/ ကို သွားပါ။

Download လုပ်ရန်အတွက် Download ထဲသို့ဝင်ပါ။

မိမိ Computer က Windows computer ဖြစ်ပါက Windows ဆိုတဲ့ခေါင်းစဉ်အောက်က Exe installer - VeraCrypt Setup 1.25.9.exe ကိုနှိပ်၍ Download လုပ်ပါ ။

Mac OS ဆိုပါက MacOs ခေါင်းစဉ်အောက်က dmg file ဖြစ်တဲ့ VeraCrypt_1.25.9.dmg ကိုနှိပ်၍ Download လုပ်ရမှာဖြစ်ပါတယ်။ ပြီးရင်တော့ OSXFuse ကိုပါ တစ်ခါထဲ Download ဆွဲရမှာဖြစ်ပါတယ်။ ပြီးရင်တော့ OSxfuse ကိုလဲ Install လုပ်ထားပါ။

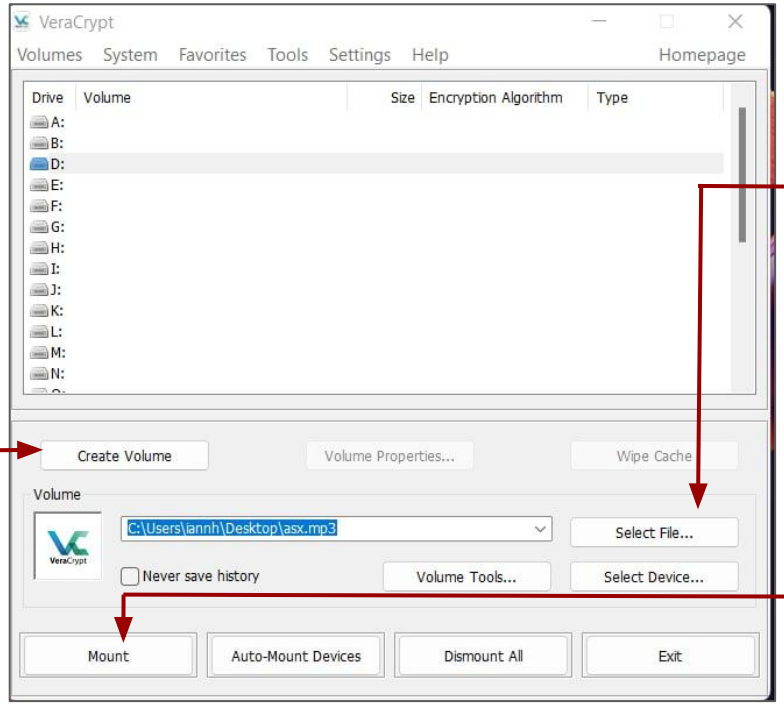
Veracrypt ကို Download ဆွဲပြီး မိမိ Computer ထဲရောက်ရှိပါက Install လုပ်လို့ရပါပြီ။

- ***Windows***:
  - EXE Installer: VeraCrypt Setup 1.25.9.exe (21.1 MB) (PGP Signature)
  - MSI Installer (64-bit) for Windows 10 and later: VeraCrypt_Setup_x64_1.25.9.msi (29 MB) (PGP Signature)
  - Portable version: VeraCrypt Portable 1.25.9.exe (20.9 MB) (PGP Signature)
  - Debugging Symbols: VeraCrypt_1.25.9_Windows_Symbols.zip (18.4 MB) (PGP Signature)
- ***macOS***:
  - macOS Mavericks 10.9 and later: VeraCrypt_1.25.9.dmg (11.7 MB) (PGP Signature)
  - **OSXFUSE** 3.10 or newer must be installed.

What is VeraCrypt

Veracrypt ကို စတင် အသုံးပြုရန်ဖွင့်ပါ။

Slot ဆိုတဲ့နေရာအောက်မှာမြင်တွေ့ရမယ့် A,B,D or 1,2,3,4 စတာတွေဟာ မိမိဖန်တီးမယ့် Virtual Drive (မိမိတည်ဆောက်လိုက်တဲ့ Encrypted Container လေးတွေကို ထည့်သွင်းပြီး ဖွင့်ရမယ့် ဘာမှမရှိတဲ့ အခန်းလွတ်လေးတွေပဲဖြစ်ပါတယ်။



Volume တွေတည်ဆောက်ပြီးတဲ့အခါ Select File နှင့် မိမိ တည်ဆောက်ထားတဲ့ Volume တွေကို ရွာဖွေရွေးချယ်ပြီး Slot တွေထဲ ထည့်ကာ ပြန်ဖွင့်ရမှာပဲဖြစ်ပါတယ်။

Create Volume ကတော့ မိမိရဲ့ အချက်အလက်တွေ သိမ်းဆည်းရန် တည်ဆောက်ရမယ့် File Container Volume တွေကိုတည်ဆောက်ရမယ့် နေရာပဲ ဖြစ်ပါတယ်။

Mount ကတော့ မိမိ password ထည့် တည်ဆောက် ထားတဲ့ Volume တွေကို Password ရိုက် ဖြည်ရန် နေရာပဲဖြစ်ပါတယ်။

Veracrypt (Standard File Container) တည်ဆောက်နည်း

File Container Volume တစ်ခု စတင်တည်ဆောက်ရန် Create Volume ကိုနှိပ်ပါ။

Create an encrypted file container ကတော့ Encrypted File Folder များတည်ဆောက်ရန် ဖြစ်ပြီး မိမိသိမ်းချင်သည့်အချက်အလက်များကို သိမ်းဆည်းဖို့ အတွက် ဖြစ်ပါတယ်။

ကျန်တဲ့ နှစ်ခုကတော့ မိမိရဲ့ Computer ထဲက Drive များကို Partition (အခန်းခွဲ) ၍ Password များခံပြီး Vera နှင့် Encrypt လုပ်ခြင်း နဲ့ Hard Disk , memory stick တွေကို Partition (အခန်းခွဲ) ၍ Password များခံပြီး Vera နှင့် Encrypt လုပ်ခြင်း တို့ဖြစ်ပါတယ်။

ဒီနေရာမှာ မိမိအချက်အလက်တွေသိမ်းဆည်းနိုင်တဲ့ Folder / File Container များတည်ဆောက်ရန် Create an encrypted file container ကို ရွေးချယ်ပါ။ Continue or Next ကို နှိပ်ပါ။

Veracrypt (Standard File Container) တည်ဆောက်နည်း

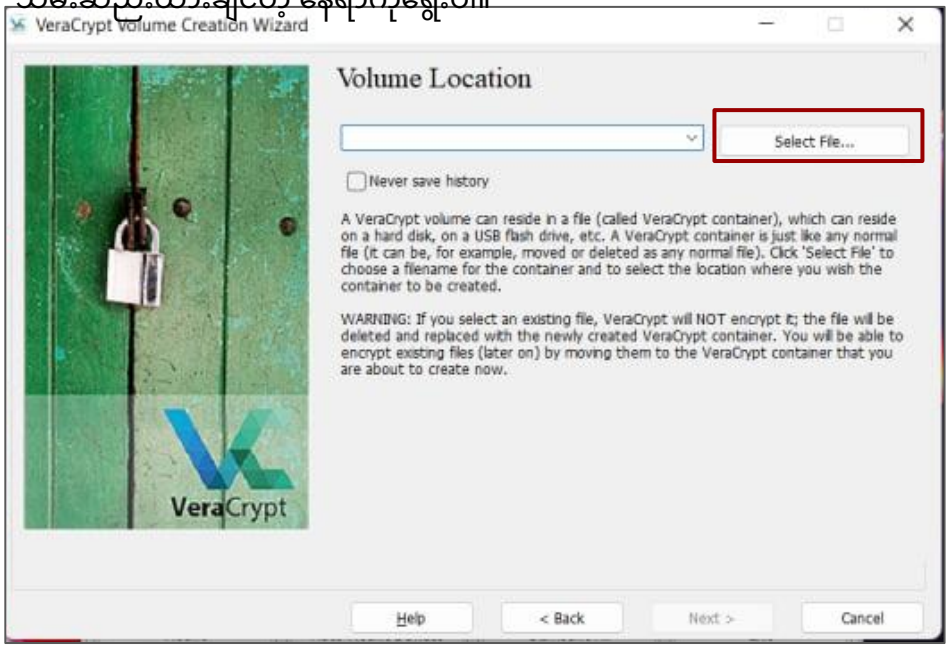
Standard File container ကတော့ အချက်အလက်တွေ ထည့်သွင်းသိမ်းဆည်းနိုင်ပြီး နေရာတကာ သယ်ဆောင်လို့ ရတဲ့မီးခံသေတ္တာလေးတွေ တည်ဆောက်တဲ့ ပုံစံဖြစ်ပါတယ်။

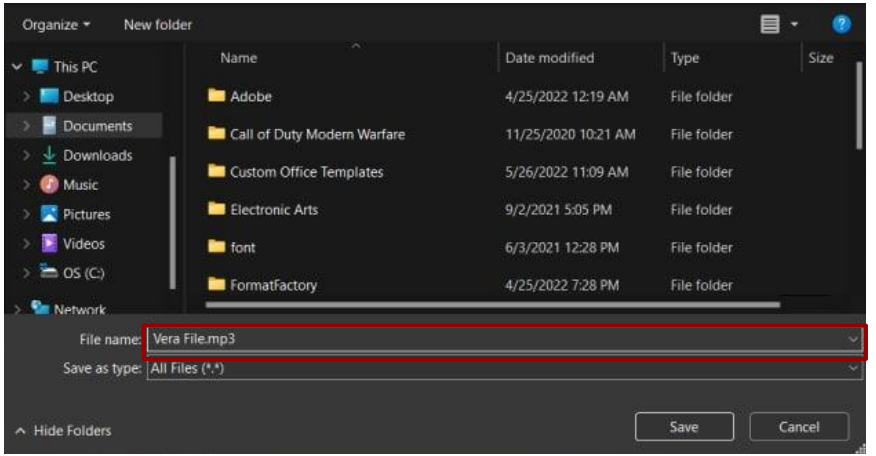
Hidden file container ကတော့ ပိုမိုလုံခြုံရန် မီးခံသေတ္တာ တစ်လုံးထဲ နောက်ထပ် မီးခံသေတ္တာတစ်လုံးကို ထည့်ပြီး နှစ်ထပ် သော့ခတ်ထားတဲ့ ပုံစံပဲဖြစ်ပါတယ်။ Hidden file container တည်ဆောက်ပုံသည် Standard Container ကို နှစ်ခါ နှစ်ထပ် ပြုလုပ်တာပဲဖြစ်ပါတယ်။

ပထမဦးစွာ **Standard file container** တည်ဆောက်ရန် ရွေးချယ်ပါ။ Next ကိုနှိပ်ပါ။

Veracrypt (Standard File Container) တည်ဆောက်နည်း

တည်ဆောက်မယ့် Container / Volume ကိုသိမ်းဆည်းရန် Volume location ကို
သတ်မှတ်ရန်လိုအပ်ပါသည်။ **Select file** ကိုနှိပ်၍ မိမိ၏ကွန်ပျူတာထဲမှာ
သိမ်းဆည်းထားချင်တဲ့ နေရာကိုရွေးပါ။



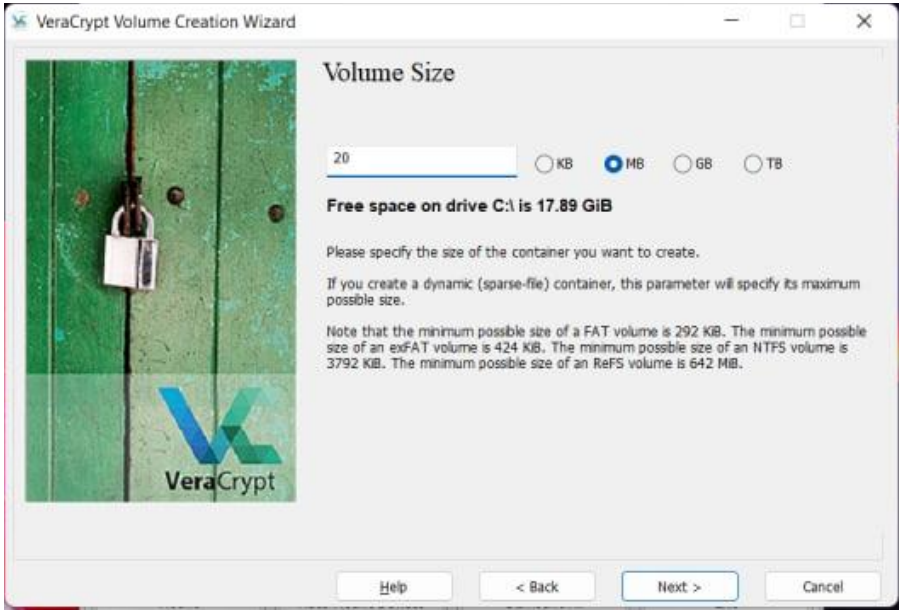


ဒီနေရာမှာ နာမည်ပေးဖို့လိုအပ်ပါတယ်။ နာမည်ပေးတဲ့နေရာမှာ နာမည်ရဲ့
နောက်မှာ ကိုယ်ထားချင်တဲ့ **File Format** ကို
ထည့်သွင်းပေးလိုက်မယ်ဆိုရင် ကိုယ်တည်ဆောက်လိုက်တဲ့ Encrypted file
container လေးဟာပေးထားတဲ့ File Format အတိုင်း file
တစ်ခုအနေနဲ့တည်ရှိနေမှာဖြစ်ပါတယ်။

ဥပမာ - kyawkyaw.mp3 ဆိုပြီး နာမည်နောက်မှာ **.MP3** လို့ပေးလိုက်ရုံနဲ့
မိမိတည်ဆောက်လိုက်တဲ့ File လေးသည် mp3 file
အနေနဲ့ရှိနေမှာဖြစ်ပါသည်။ အဲ့ဒီလို **မိမိနှစ်သက်ရာ mp3 / mp4 / pdf / jpg
စသဖြင့် extension များပြောင်း၍ file container များကို**

Veracrypt (Standard File Container) တည်ဆောက်နည်း

File Location ရွေးချယ်ပြီး Next ကိုဆက်နှိပ်ပြီးရင်တော့ Encryption Options ၏ Encryption Algorithm တွင် **AES** ကိုရွေး၍ Next ကိုဆက်နှိပ်ပါ။



Volume Size တွင် မိမိ ပြုလုပ်ချင်တဲ့ Folder size ကိုယ့် ထည့်ချင်တဲ့ အချက် အလက်တွေရဲ့ ပမာဏ နှင့် **ကိုယ့်ကွန်ပျူတာမှာကျန်တဲ့ Storage ပမာဏကို မူတည်ပြီး size သတ်မှတ်ပါ။** ဥပမာ မိမိထည့်ချင်တဲ့ အချက်အလက်တွေက 1GB ကျော်ကျော်လောက်ရှိတယ်ဆိုရင် Volume Size ကို 1.5 GB လောက်ထားလိုက်လို့ရပါတယ်။

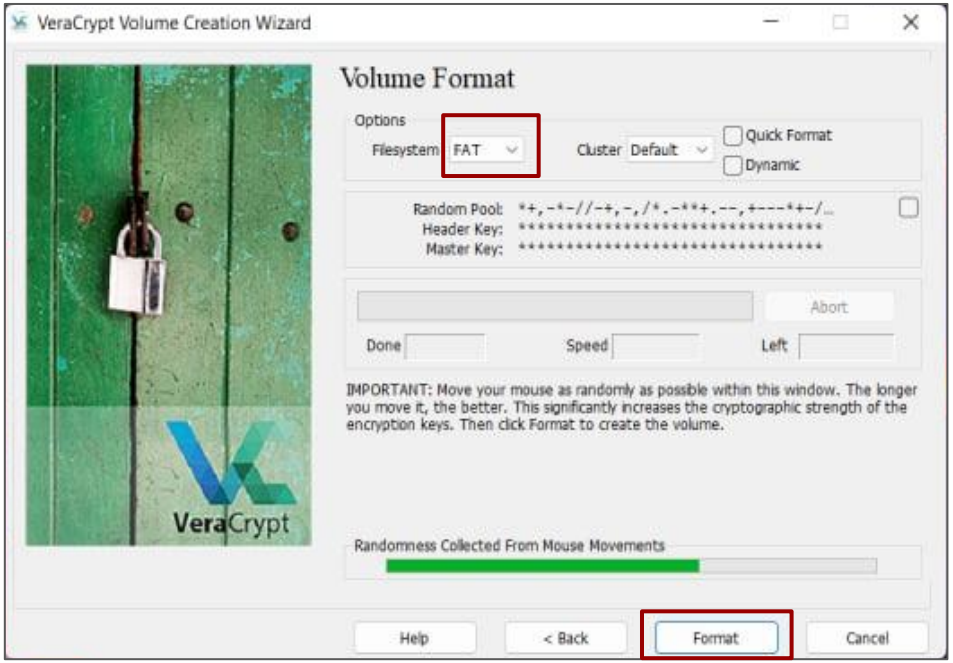
Veracrypt (Standard File Container) တည်ဆောက်နည်း

File Container ကို သော့ခတ်ရန် **Password** ထည့်သွင်းပါ။ ဒီနေရာမှာ Password သည် အရေးကြီးပါတယ်။ **မေ့သွားပါက လုံးဝ ပြန်ယူ / ပြန် Recovery လုပ်လို့မရနိုင်ပါ။** မိမိလုံခြုံရေးပေါ်မူတည်ပြီး လိုအပ်သလို Key File များလဲ ထည့်သွင်းနိုင်ပါတယ်။

Keyfile ထည့်မယ်ဆိုရင်တော့ မိမိ ကြိုက်နှစ်သက်ရာ ဓာတ်ပုံ ၊ ဗီဒီယိုများကို တွဲထည့်လို့ရပါတယ်။

သို့သော် veracrypt နှင့်တည်ဆောက်ထားတဲ့ မိမိရဲ့ file container ကိုဖွင့်တိုင်း keyfile ကိုပါ မဖြစ်မနေ ပြန်ထည့်ပေးရမှာဖြစ်ပါတယ်။ Keyfile မရှိလဲ လုံးဝ ဖွင့်လို့မရနိုင်ပါ။ နှစ်ဆင့်ခံလုံခြုံရေး သဘော ပင် ဖြစ်သည်။

Veracrypt (Standard File Container) တည်ဆောက်နည်း



နောက်တစ်ဆင့်အနေနဲ့ တည်ဆောက်ထားတဲ့ file container ကို ရှင်းလင်းရန် Format Option တွင် **FAT** ထားပါ ။

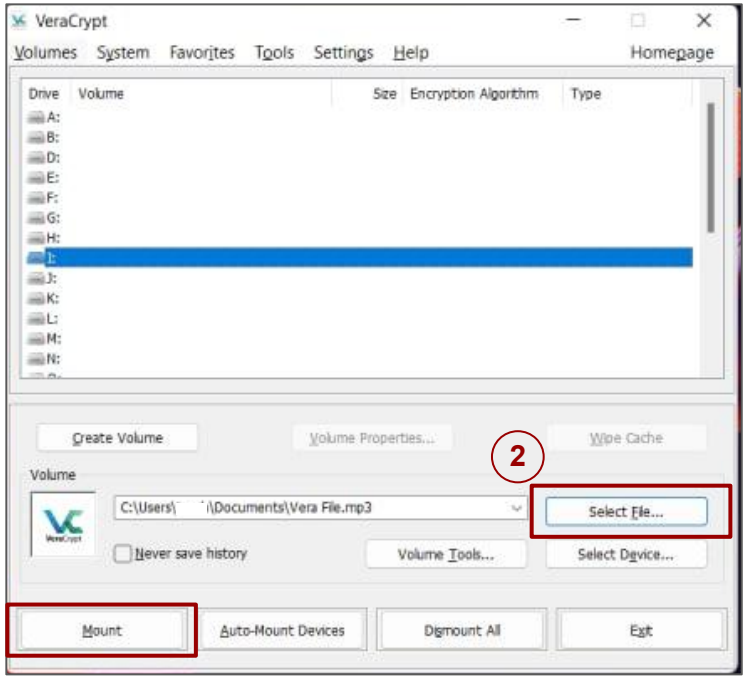
FAT , EXFAT , Mac OS extended စသဖြင့် မိမိ ဖွင့်မည့် operating system ပေါ်မူတည်ပြီးရွေးချယ်နိုင်ပါတယ်။

FAT နှင့် EXFAT သည် မိမိ file container ကိုပြန်ဖွင့်တဲ့အခါ Window ကွန်ပျူတာမှာကော MAC OS ကွန်ပျူတာ များမှာပါဖွင့်နိုင်တဲ့အတွက် အဆင်ပြေဆုံးဖြစ်ပါတယ်။

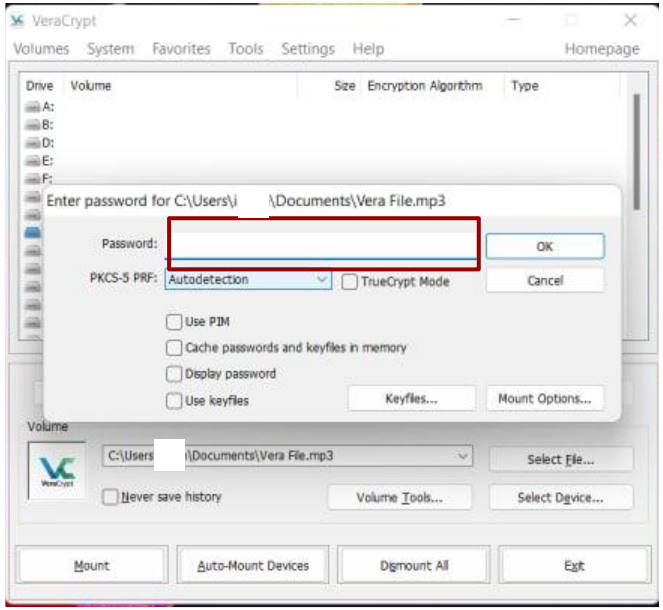
ပြီးရင်တော့ Format လုပ်ပါ။ Format လုပ်ရာမှာ အစိမ်းရောင် ဘားတန်းလေး အမြန်တတ်ရန်အတွက် Mouse ကိုပါလိုက်ရွေ့လျားပေးပါ။ အစိမ်းရောင်လေး အကုန်ပြည့်သွားပြီးဆိုရင်တော Format ကိုနှိပ်ပါ။ Format ချပြီးရင်တော့ Encrypted file container တည်ဆောက်ခြင်းပြီးဆုံးပြီဖြစ်ပါတယ်။

Encrypted Container ထဲ Data အချက်အလက်များ ထည့်၍ သိမ်းဆည်းခြင်း

မိမိ သိမ်းဆည်းချင်တဲ့ Data အချက်အလက်တွေကို သိမ်းဆည်းရန် မိမိတည်ဆောက်ခဲ့တဲ့ Container ကို Veracrypt နှင့် ပြန်လည်ဖွင့်လှစ်ရန်လိုအပ်ပါသည်။ Veracrypt ကိုဖွင့်ပါ။ ကြိုက်နှစ်သက်ရာ Slot ကိုရွေးချယ်ပါ။



Select file ကိုနှိပ်၍ မိမိဖန်တီးတည်ဆောက်ထားခဲ့တဲ့ container အား သွားရောက်ရွေးချယ်ဖွင့်လှစ်ပါ။

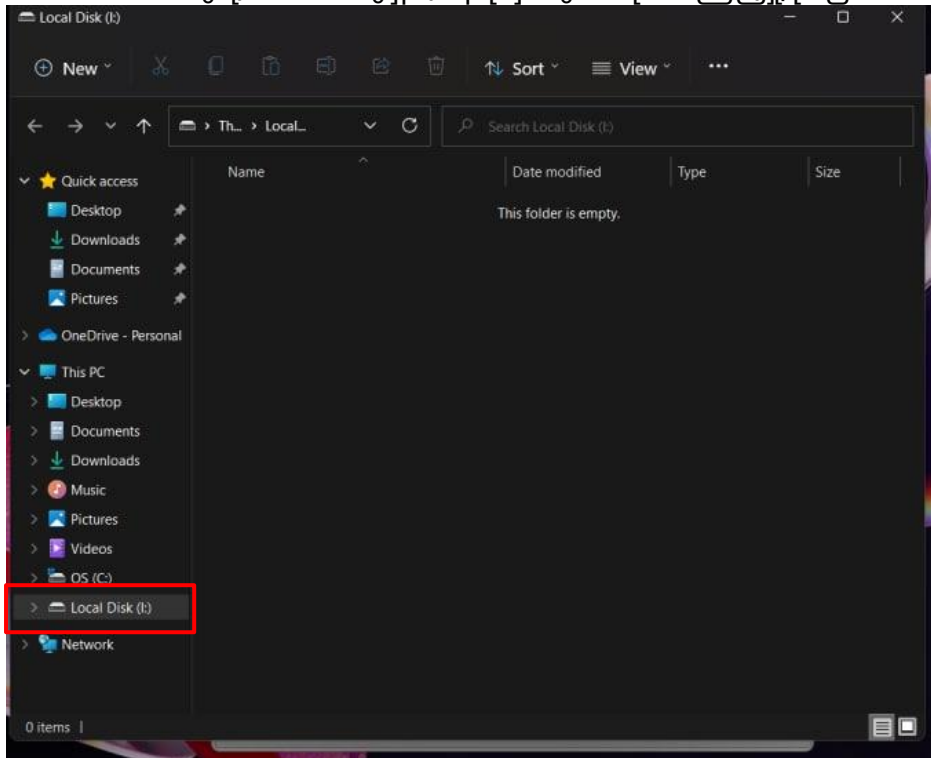


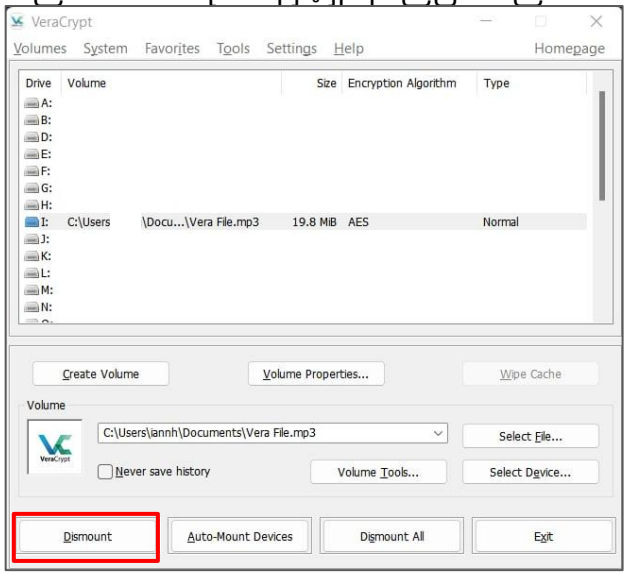
Select file ရဲ့ ဘယ်ဘက်ဘေးက box ထဲတွင် မိမိရွေးချယ်ထားတဲ့ File လေး ဝင်ရောက် သွားပြီဆိုလျှင် Mount ကိုနှိပ်ပါ။

Mount သည် မိမိ File ကို ပြန်ဖွင့်ရန်ဖြစ်ပြီး Mount ကို နှိပ်ပါက Password ထည့်ခိုင်းမည်ဖြစ်သည်။ မိမိ File Container တည်ဆောက်စဉ်တုန်းက ပြုလုပ်ထည့်သွင်းခဲ့တဲ့ Password ကို ထည့်ပါ။

Encrypted Container ထဲ Data အချက်အလက်များ ထည့်၍ သိမ်းဆည်းခြင်း

ဒါဆိုရင် File Container လေးပွင့်သွားမည်ဖြစ်ပြီး မိမိ ထည့်သွင်းသိမ်းဆည်းထားချင်တဲ့ အချက်အလက်များကို ထည့်သွင်းပါ။ File Container ပွင့်နေကြောင်းကို
မိမိ၏ My computer တွေရဲ့ Drive တွေရှိတဲ့နေရာမှာသွားရောက် ကြည့်ရှုနိုင်ပြီး File Container သည် Drive တစ်ခုအနေနှင့်ရှိနေမည်ဖြစ်သည်။





အချက်အလက်များ သိမ်းဆည်းပြီးပါက Veracrypt မှ Dismount ကိုပြန်နှိပ်၍ File Container ကိုပိတ်ပါ။ Veracrypt နှင့် password ဖွင့်၍ သာ ကြည့်ရှုနိုင်ပြီး သာမန် Click နှိပ်၍ ကြည့်နိုင်မှာမဟုတ်ပါ။

Hidden File Container တည်ဆောက်ခြင်း

Hidden File Container တည်ဆောက်ခြင်းသည် Standard ကို နှစ်ဆင့် နှစ်ခါလုပ်ဆောင်ခြင်းဖြစ်ပြီး မိမိ အချက်အလက်များကို သိမ်းဆည်းရန် အလွှာနှစ်ထပ်ခံထားသည့်ပုံစံဖြစ်သည်။

ပထမ အလွှာ Outer Volume ကို Standard Container ပြုလုပ်သလို အဆင့်ဆင့် တည်ဆောက်ပြီး ဒုတိယအလွှာ Hidden volume ကို ထပ်မံတည်ဆောက်ရမည်ဖြစ်ပြီး ထူးခြားချက်ကတော့ ပထမ အလွှာ outer Volume မှာ အချက်အလက်တွေသိမ်းဆည်းလို့ရသလို ဒုတိယအလွှာ hidden volume မှာလဲ အချက်အလက်တွေကို ပိုမိုလုံခြုံစွာသိမ်းဆည်းနိုင်ပါသည်။ ပြန်ဖွင့်သည့်အခါမှာလဲ သက်ဆိုင်ရာ Volume ရဲ့ password ကိုနှိပ်ပြီးမိမိ သွားချင်တဲ့ outer volume , hidden volume များကိုတိုက်ရိုက်ဖွင့်နိုင်ပါသည်။

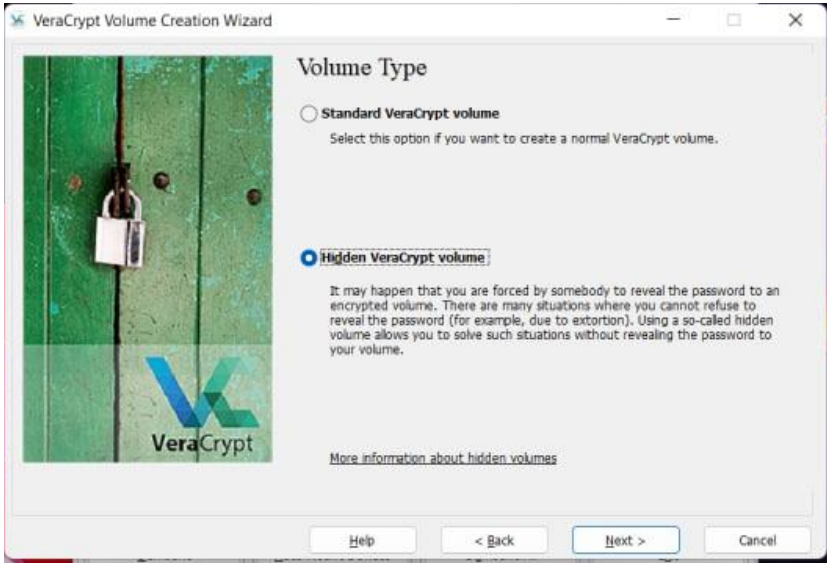
Hidden File Container တည်ဆောက်ရန်

File Container Volume တစ်ခု စတင်တည်ဆောက်ရန် Create Volume ကိုနှိပ်ပါ။

Create an encrypted file container ကို ရွေးချယ်ပါ။ Continue or Next ကို နှိပ်ပါ။

Hidden File Container တည်ဆောက်ခြင်း

Hidden Veracrypt Volume ကိုရွေးပါ။



တည်ဆောက်မယ့် Container / Volume ကိုသိမ်းဆည်းရန် Volume location ကို သတ်မှတ်ရန်လိုအပ်ပါသည်။ Select file ကိုနှိပ်၍ မိမိ၏ကွန်ပျူတာထဲမှသိမ်းဆည်း ထားချင်တဲ့ နေရာကိုရွေးပါ။ နာမည်ပေးရာတွင် File ကိုကိုယ်ရောင်ဖျောက်သိမ်းဆည် ရန် နာမည်၏ နောက်တွင် ကြိုက်နှစ်သက်ရာ file format ထည့်၍ နာမည်ပေးလိုက်ပါ။

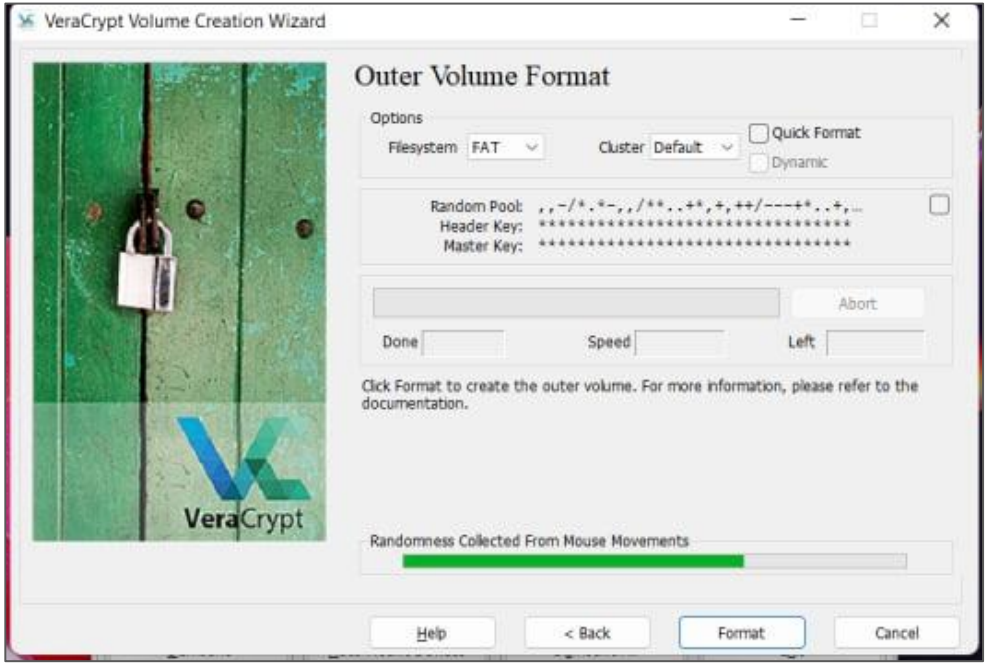
Hidden File Container တည်ဆောက်ခြင်း

Encryption algorithm တွင် AES ကိုရွေးချ၍ Next ကိုဆက်နှိပ်ပါ။ Volume Size တွင် မိမိ ပြုလုပ်ချင်တဲ့ Folder size ကို ကိုယ် ထည့်ချင်တဲ့ အချက်အလက်တွေရဲ့ ပမာဏ နှင့် ကိုယ့်ကွန်ပျူတာမှာကျန်တဲ့ Storage ပမာဏကိုမူတည်ပြီး size သတ်မှတ်ပါ။ **အခုသတ်မှတ်မယ့် Volume သည် hidden အလွှာအတွက်ကော outer အလွှာအတွက်ပါ သတ်မှတ်ရမှာဖြစ်တဲ့အတွက် တစ်ခါတည်း Volume Size ကြီးကြီးသတ်မှတ်ပေးပါ။**

ပထမဆုံး အနေနဲ့ **Outer အလွှာအတွက် password အရင် သတ်မှတ်ရပါမည်**။ Password သတ်မှတ်ပြီးတာနဲ့ next ကို ဆက်နှိပ်လိုက်ပါ။

Hidden File Container တည်ဆောက်ခြင်း

နောက်တစ်ဆင့်အနေနဲ့ တည်ဆောက်ထားတဲ့ file container ကို ရှင်းလင်းရန် Format Option တွင် **FAT** ထားပါ ။ပြီးရင်တော့ Format လုပ်ပါ။ Format လုပ်ရာမှာ အမြန်တတ်ရန်အတွက် Mouse ကိုပါလိုက်ရွေ့လျားပေးပါ။ Format ချပြီးရင်တော့ outer အလွှာအတွက် တည်ဆောက်ခြင်းပြီးဆုံးပြီဖြစ်ပါတယ်။



open outer volume ဖွင့်၍ outer ထဲမှာ မိမိထည့်ချင်တာတွေကို တစ်ခါတည်းထည့်ထားလို့ရသလို နောက်မှ outer အလွှာရဲ့ password ကို ထည့်၍ ပြန်ဖွင့်နိုင်ပါသည်။

Hidden File Container တည်ဆောက်ခြင်း

Hidden volume ကိုဆက်၍ တည်ဆောက်ရန်လိုအပ်ပါသည်။ Next ကိုဆက်နှိပ်ပါ။

Encryption Algorithm မှာ AES ပဲထား၍ Next ကိုဆက်နှိပ်ပါ။

Password ပေးရာတွင် outer volume နဲ့မတူညီတဲ့ password ကိုပေးရန်လိုအပ်ပါသည်။ သို့မှသာ မိမိထည့်သွင်းတဲ့ password ပေါ်မူတည်ပြီး Outer or hidden volume များပွင့်မှာဖြစ်ပါသည်။

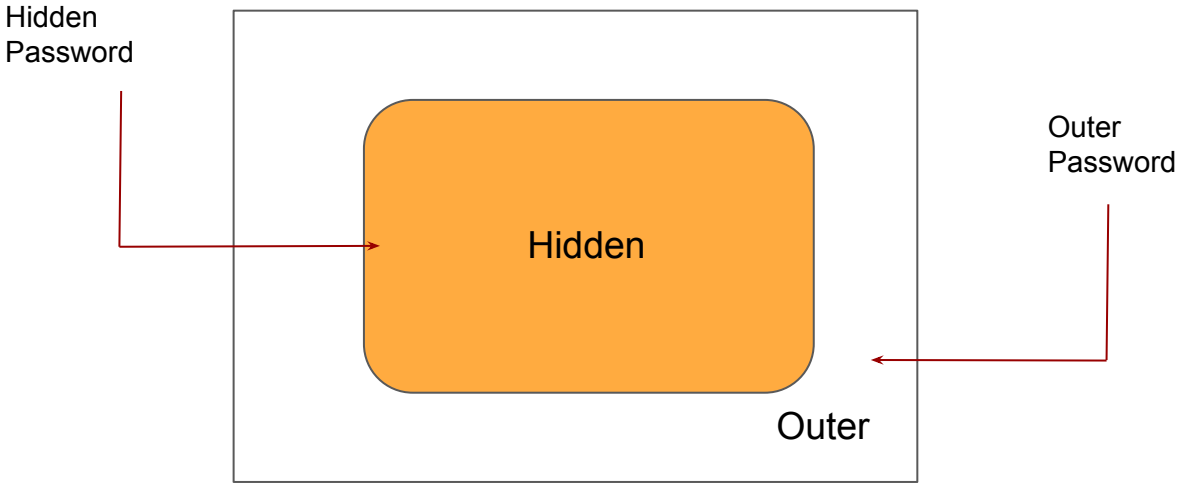
Hidden File Container တည်ဆောက်ခြင်း

အခု သတ်မှတ်ပေးရမယ့် Volume size သည် outer မှာသတ်မှတ်ထားခဲ့တာထက်နည်းရမည်ဖြစ်သည်။
ကြက်ဥ တစ်လုံးလိုပဲ အကာထဲမှာမှ အနှစ်အတွက် နေရာ သတ်မှတ်ပေးရမယ့်ပုံစံမျိုးဖြစ်ပါသည်။

ပြီးရင်တော့ FAT နဲ့ Format ချလိုက်ပါ။ ဒါဆိုရင် Hidden Encrypted file container
တည်ဆောက်ခြင်းပြီးဆုံးပြီဖြစ်ပါတယ်။

Encrypted Container ထဲ Data အချက်အလက်များ ထည့်၍ သိမ်းဆည်းခြင်း

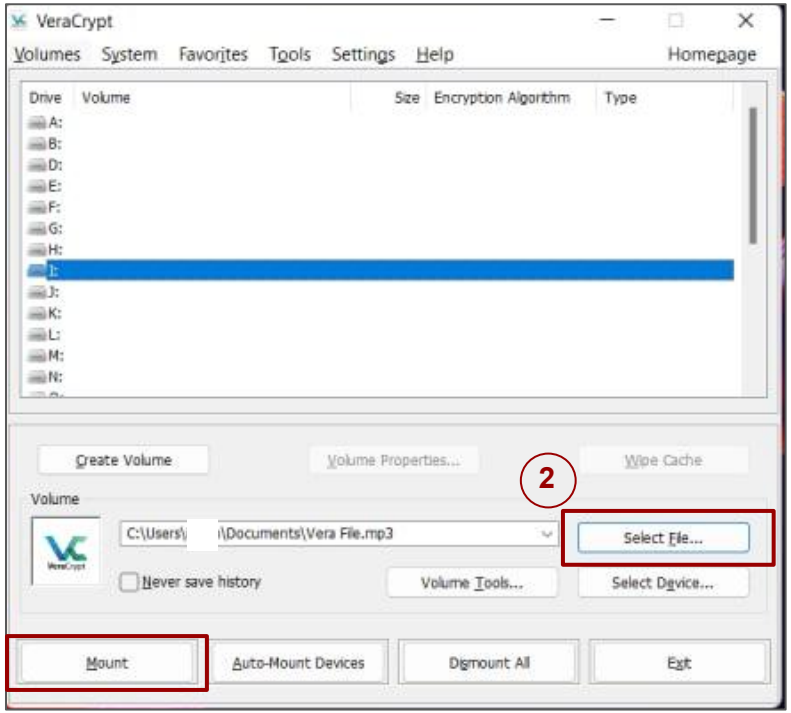
မိမိ သိမ်းဆည်းချင်တဲ့ Data အချက်အလက်တွေကို သိမ်းဆည်းရန် Standard file container ဖွင့်သလိုပဲ မိမိတည်ဆောက်ခဲ့တဲ့ Container ကို Veracrypt နှင့် ပြန်လည်ဖွင့်လှစ်ရန်လိုအပ်ပါသည်။



ဒီနေရာမှာ အဓိကအချက်ကတော့ Outer Volume မှာပေးခဲ့တဲ့ Password ကိုထည့်သွင်းရင် outer volume က ပွင့်မှာဖြစ်ပြီး Hidden volume ရဲ့ password ကိုထည့်သွင်းပါက Hidden volume ပွင့်မည်ဖြစ်ပါသည်။

Encrypted Container ထဲ Data အချက်အလက်များ ထည့်၍ သိမ်းဆည်းခြင်း

မိမိ သိမ်းဆည်းချင်တဲ့ Data အချက်အလက်တွေကို သိမ်းဆည်းရန် Standard file container ဖွင့်သလိုပဲ မိမိတည်ဆောက်ခဲ့တဲ့ Container ကို Veracrypt နှင့် ပြန်လည်ဖွင့်လှစ်ရန်လိုအပ်ပါသည်။



Select file နှင့် မိမိ file ကိုရွေးပါ။ mout ကိုနှိပ်၍ password ဖြည်ပါ။

ကိုယ့်ရဲ့ လိုအပ်ချက်ပေါ်မူတည်၍ Outer နဲ့ Hidden volume တွေကို အချက်အလက်များထည့်သွင်း၍ လုံခြုံအောင် သိမ်းဆည်းထားနိုင်ပါသည်။

ဒီလိုနည်းနှင့် Standard Encrypted File Container ၊ Hidden Encrypted File Container များ တည်ဆောက်၍ မိမိရဲ့ ထိရှလွယ်တဲ့ အချက်အလက်များ
ကို လုံခြုံစိတ်ချစွာသိမ်းဆည်းထားနိုင်ပါသည်။

Full Disk Encryption (သို့) Partition ခဲခြင်း

Full Disk Encryption (သို့) Partition ခွဲခြင်း

ထိရှလွယ်တဲ့ ဒေတာတွေကို Volume တစ်ခုတည်းမှာသိမ်းထားရုံတင်မကပဲ.. မိမိရဲ့ ကွန်ပျူတာထဲမှာရှိတဲ့ Drive Storage ထဲက Storage တစ်ဝက်ကို အပိုင်းခွဲပြီး Encrypt လုပ်နိုင်သလို၊ မိမိတို့သုံးနေတဲ့ External Hard Drive၊ Memory Stick တစ်ခုလုံးကို Encrypted လုပ်နိုင်သလို အပိုင်းလေး ပိုင်းပြီးလည်း Encrypt လုပ်နိုင်မှာပါ။ Hard Disk ထည့်လိုက်တာနဲ့ Partition ခွဲပြီး Encrypt လုပ်ထားတဲ့အပိုင်းကို ဖျောက်ထားပေးမှာ ဖြစ်ပြီး Veracrypt နဲ့သာ ဖွင့်လို့ ရနိုင်တော့မှာပါ။

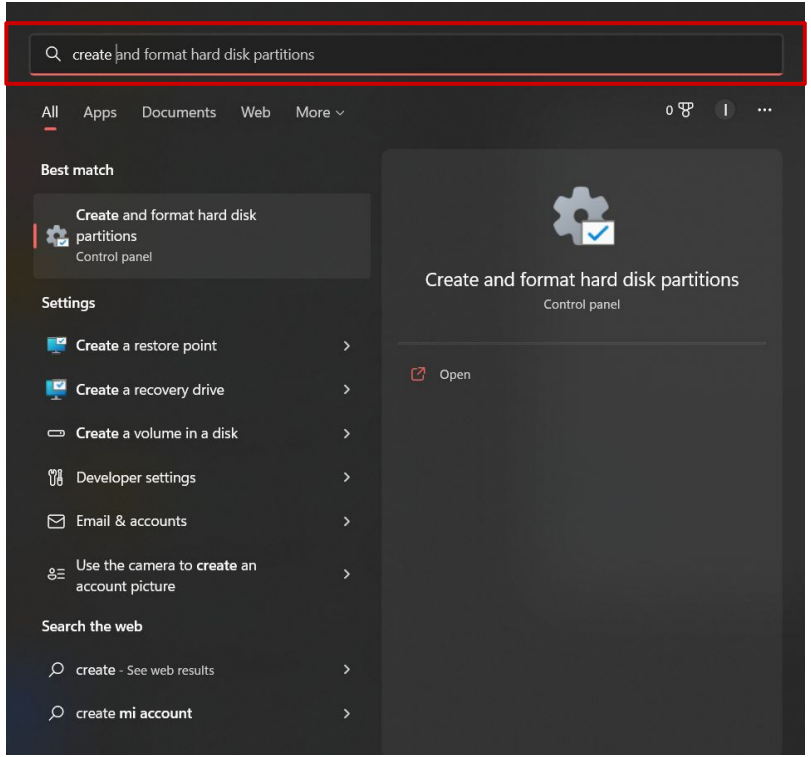
- **Partition မခွဲခင် (သို့) Full Disk တစ်ခုလုံးကို Encrypt မလုပ်ခင် မိမိအတွက် အရေးကြီးသော ဒေတာများကို မဖြစ်မနေ Backup လုပ်ထားရန်လိုအပ်ပါသည်။**
- မိမိရဲ့ External Hard Drive ရဲ့ File System ကတော့ NTFS File System မဟုတ်ဘူးဆိုရင် မိမိရဲ့ External Hard Drive ကို အပိုင်းခွဲ၍ Encrypted လုပ်လို့ရနိုင်မည်မဟုတ်ပါ။
- အဲ့ဒါကြောင့် Hard Disk သို့ External Hard Drive ကို မိမိစိတ်ကြိုက် အပိုင်းခွဲနိုင်ဖို့ Hard Disk / External Hard Drive တွင်ရှိနှင့်ပြီးသော ဒေတာများကို အရင်ဖျက်ထားသင့်သည်။

Full Disk Encryption (သို့) Partition ခွဲခြင်း

Partition ခွဲခြင်းဆိုသည်မှာ မိမိ၏ မိမိကွန်ပျူတာထဲမှာရှိသော Internal Hard Diskı External Hard Drive (သို့) Memory Stick (USB) ကို မိမိလိုအပ်သော Storage တစ်ခုသတ်မှတ်ပိုင် အကန့်တစ်ကန့် ကန့်လိုက်ခြင်း (သို့) အပိုင်းပိုင်း လိုက်ခြင်းဖြစ်သည်။ ဥပမာ မိမိမှာ 16GB USB ကို 8GB နှစ်ပိုင်းခွဲလိုက်ခြင်းဖြစ်သည်။

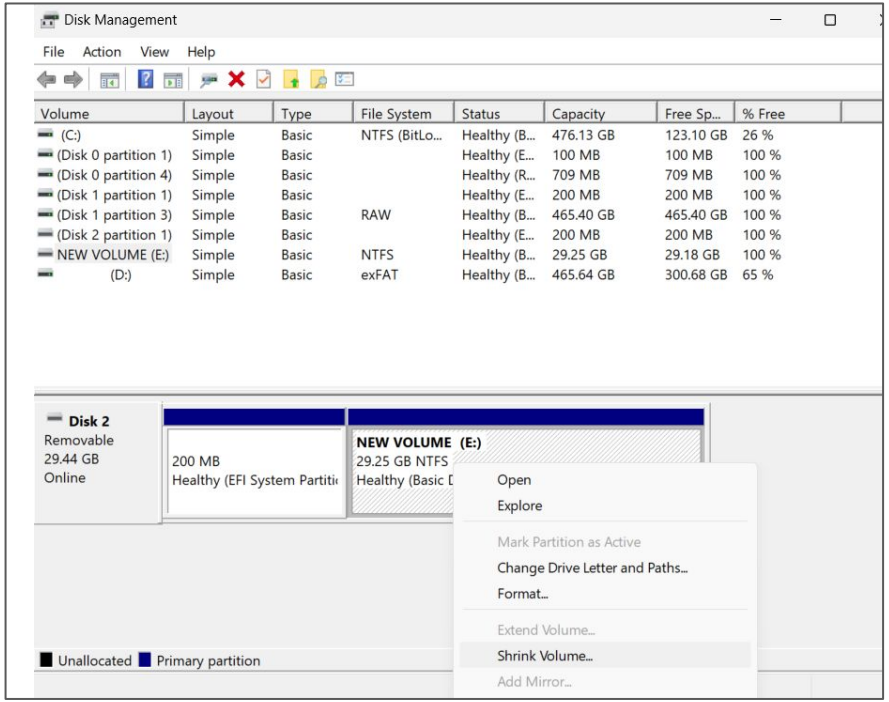
Partition ပြုလုပ်ဖို့ရန်အတွက်

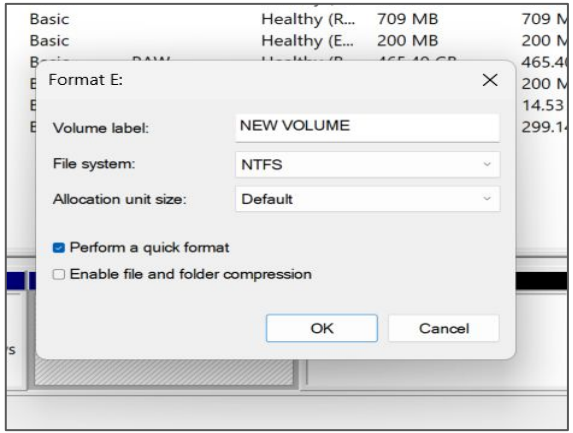
1. **“Create and Format hard disk partitions”** ကို Keyboard ပေါ်က **Windows key နှိပ်ပီး Windows Search ကိုရှာနိုင်သလို Computer Screen ဘယ်ဘက်ထောင့်က Window Logo ကိုနှိပ်ပြီးလည်းရှာနိုင်ပါတယ်။**

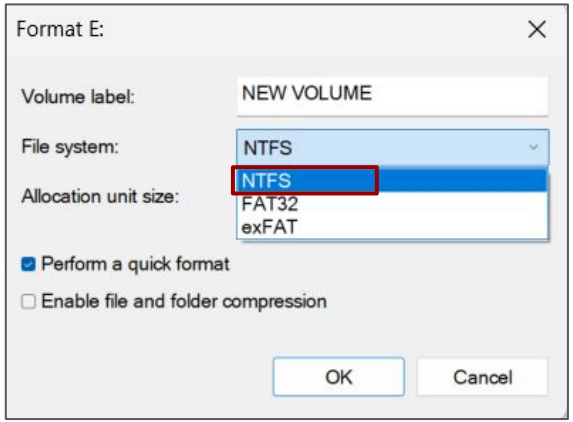


NTFS မဟုတ်ရင် Format အရင်ချရန်

- (မိမိရဲ့ External hard drive ရဲ့ file system က NTFS မဟုတ်နေဘူးဆိုရင် Format အရင်ချဖို့လိုပါလိမ့်မယ်။
- Format ကိုနှိပ်ပါ။



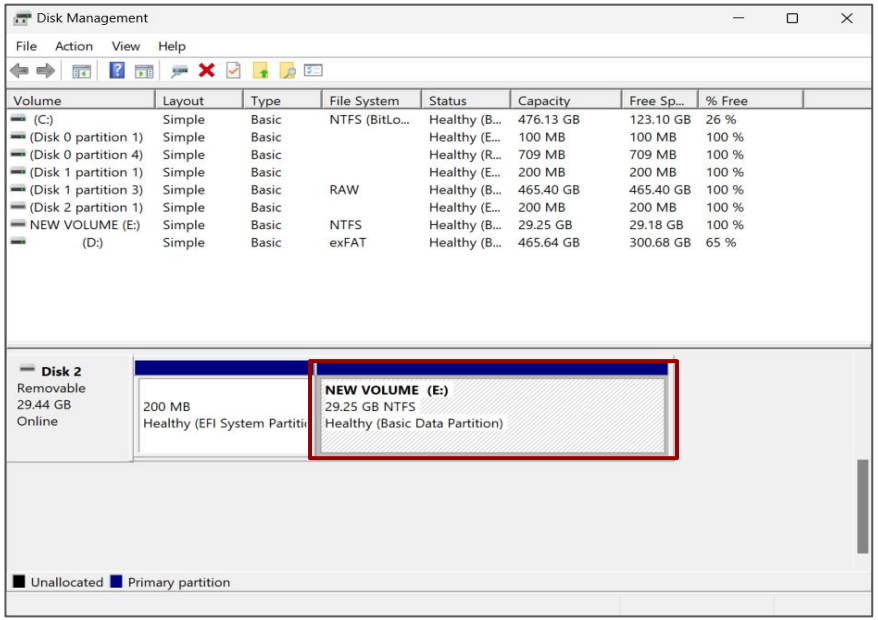


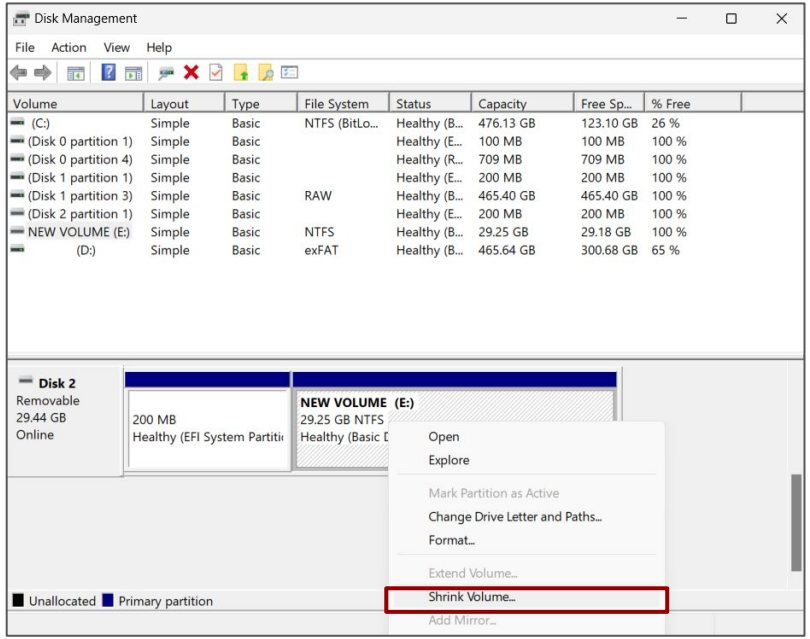


File System မှာ NTFS ကိုနှိပ်ပါ။ OK ကိုနှိပ်ပြီး Format ချပါ။

Hard Disk သို့မဟုတ် Memory Stick ကို Partition ခွဲခြင်း

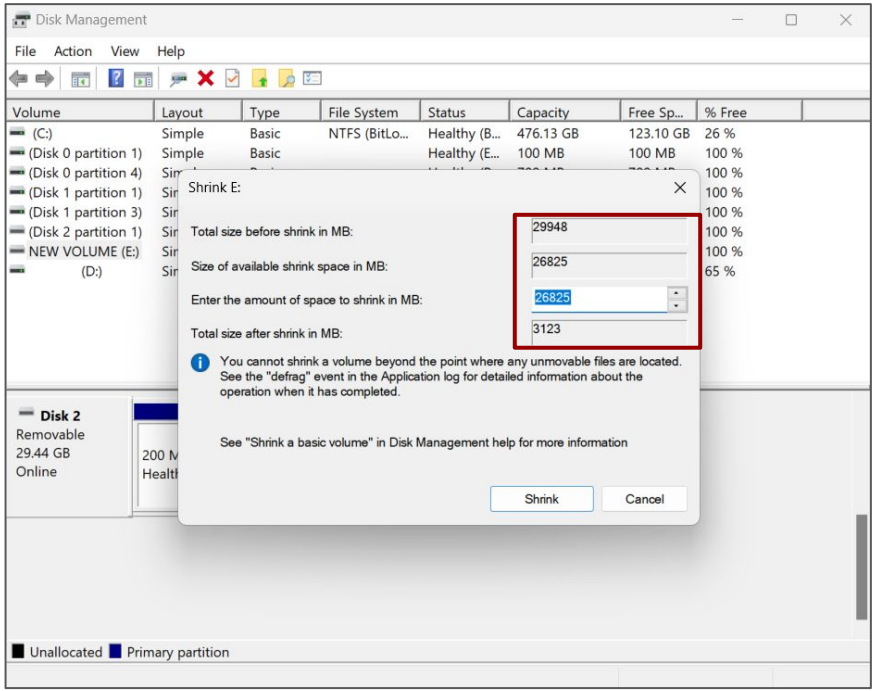
1. မိမိ ချိန်ညှိချင်တဲ့မိမိရဲ့ external hard disk သို့မဟုတ် Memory Stick ကိုရွေးချယ်ပြီး **right click နှိပ်ပါ။**





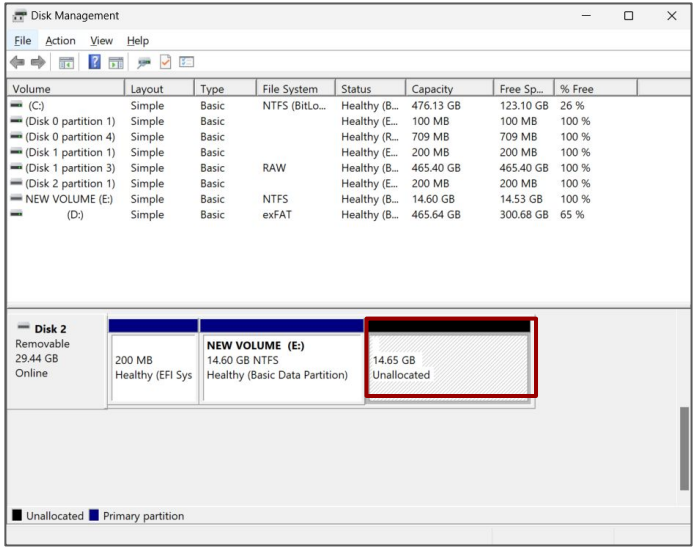
2. Right click နှိပ်ပြီး Shrink Volume ကိုနှိပ်ပါ။ (မိမိရဲ့ External hard drive ရဲ့ file system က NTFS မဟုတ်နေဘူးဆိုရင် Shrink Volume က ခဲရောင်ဖြစ်နေပီးနှိပ်လို့ရမှာ မဟုတ်ပါဘူး)

Manage Partitions (အကန့်ခွဲပြီး Storage ကိုစီမံခန့်ခွဲခြင်း)



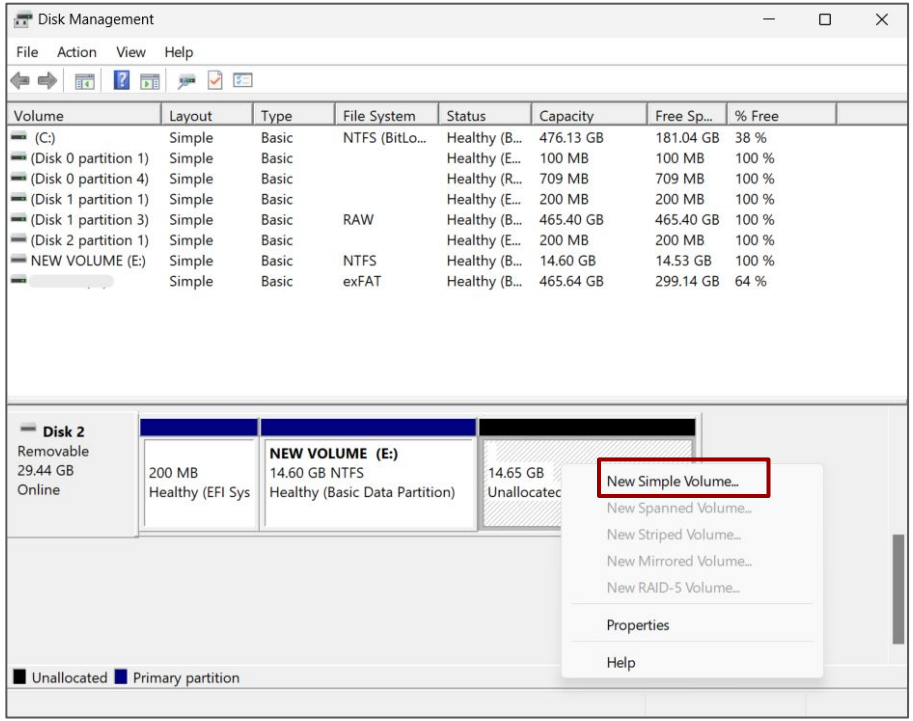
မိမိစိတ်ကြိုက် size ကိုခွဲခြမ်းလို့ရပါတယ်။

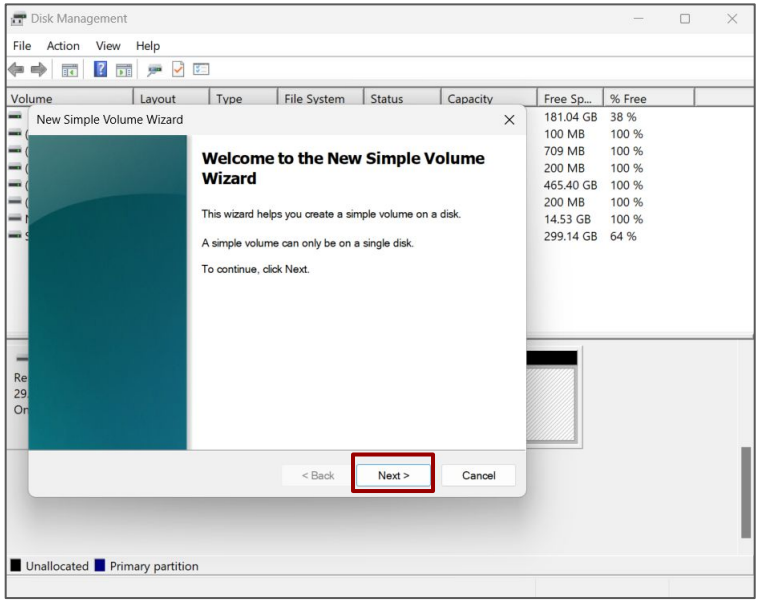
Shrink လုပ်ပြီးပြီဆိုရင် unallocated partition ဆိုပီးပေါ်လာပါလိမ့်မယ်။ **Unallocated partition က file system မသတ်မှတ်ရသေးခင် အခြေအနေဖြစ်ပါတယ်။** File system မသတ်မှတ်မပေးချင်း Mount လို့ရမှာမဟုတ်ပါဘူး။



Manage Partitions (အကန့်ခွဲပြီး Storage ကိုစီမံခန့်ခွဲခြင်း)

Unallocated Volume ကို Right Click နှိပ်ပြီး New Simple Volume ကိုနှိပ်ပါ။

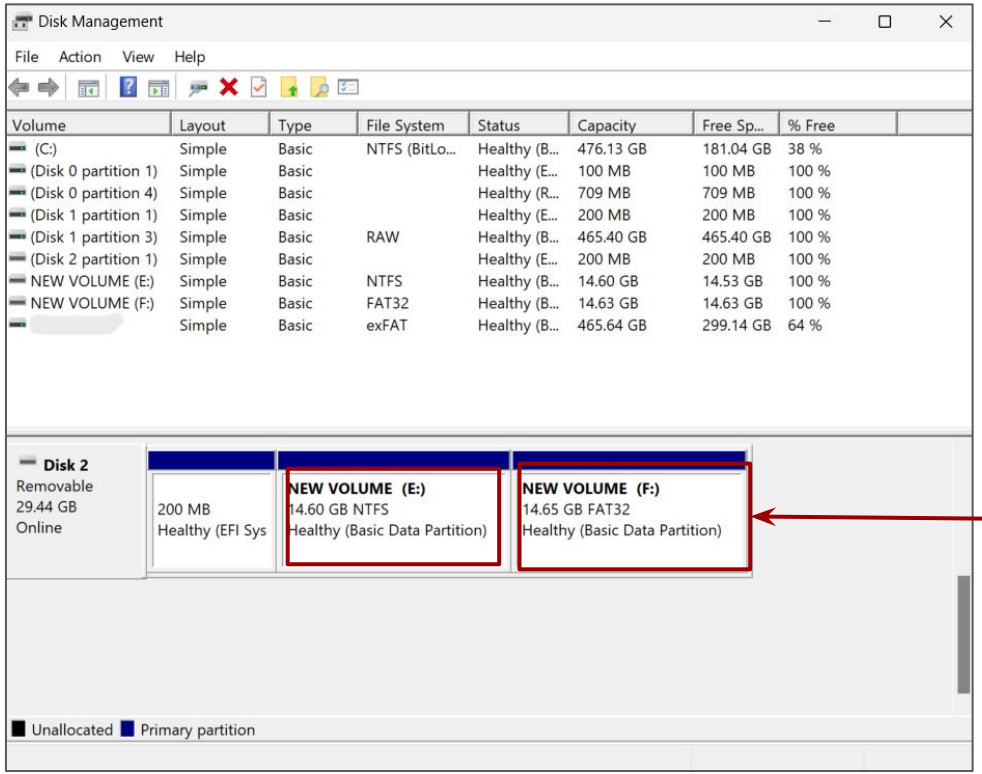




နောက်စာမျက်နှာများကို ဆက်တိုက် Next ကိုနှိပ်ပေးပါ။

Manage Partitions (အကန့်ခွဲပြီး Storage ကိုစီမံခန့်ခွဲခြင်း)

Next ဆက်တိုက်နှိပ်ပြီးပါက နောက်ဆုံးတွင် partition ပေါ်လာမည်ဖြစ်သည်။



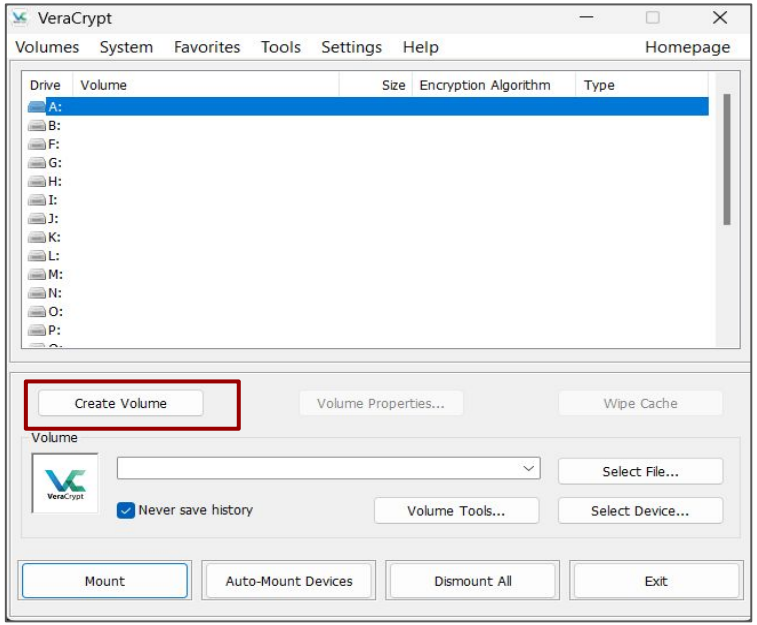
ဒီအဆင့်သို့ရောက်ပြီးပါက Partitionခွဲ ခြင်းပြီးဆုံးပြီဖြစ်ပါသည်။ Veracrypt App ကိုဖွင့်လို့ရပါပြီ။

Partition ခွဲလိုက်သည့်အတွက် Volume နှစ်ခု ကွဲသွားတာကိုမြင်တွေ့ရမည်ဖြစ်သည်။

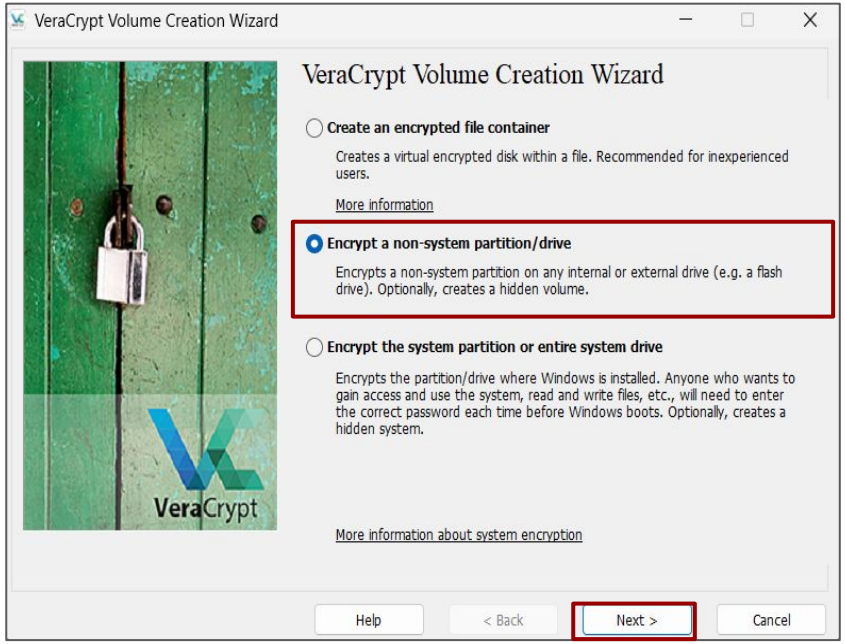
External hard-drive or USB ကို Encrypt လုပ်ခြင်း

မိမိ အသုံးပြုမည့် External Hard Drive (သို့) Memory Stick (USB) တစ်ခုလုံးကို Encrypt လုပ်ခြင်း ကိုဒီနေရာမှာ လုပ်ပြသွားမှာဖြစ်ပါတယ်။

1. **Create Volume ကိုနှိပ်ပြီး “Encrypt a non-system partition/drive” ကိုရွေးချယ်ပါ။**

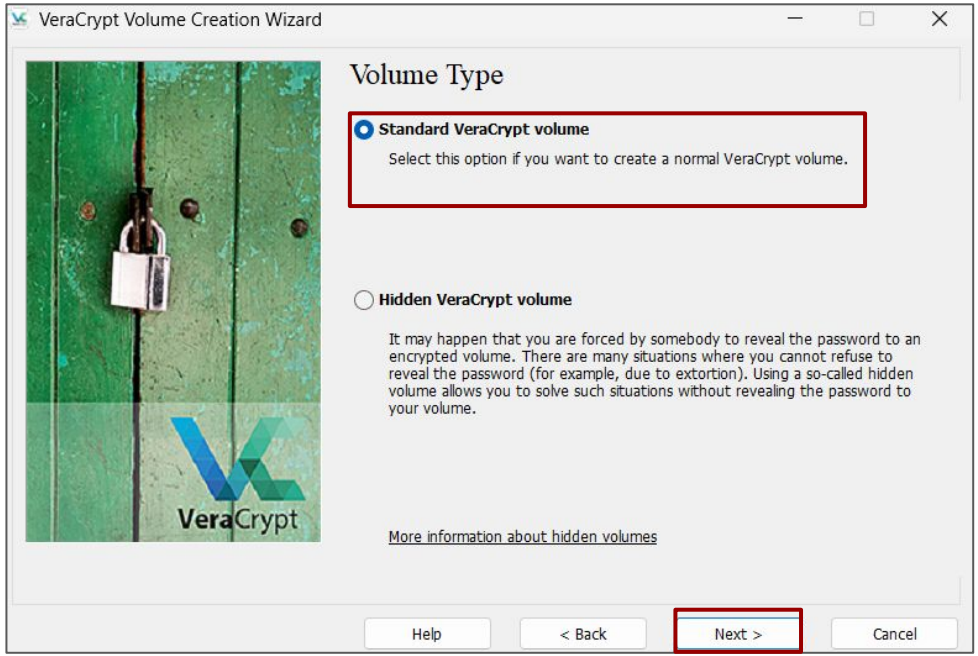


2. **Next ကိုနှိပ်ပါ။**



External hard-drive or USB ကို Encrypt လုပ်ခြင်း

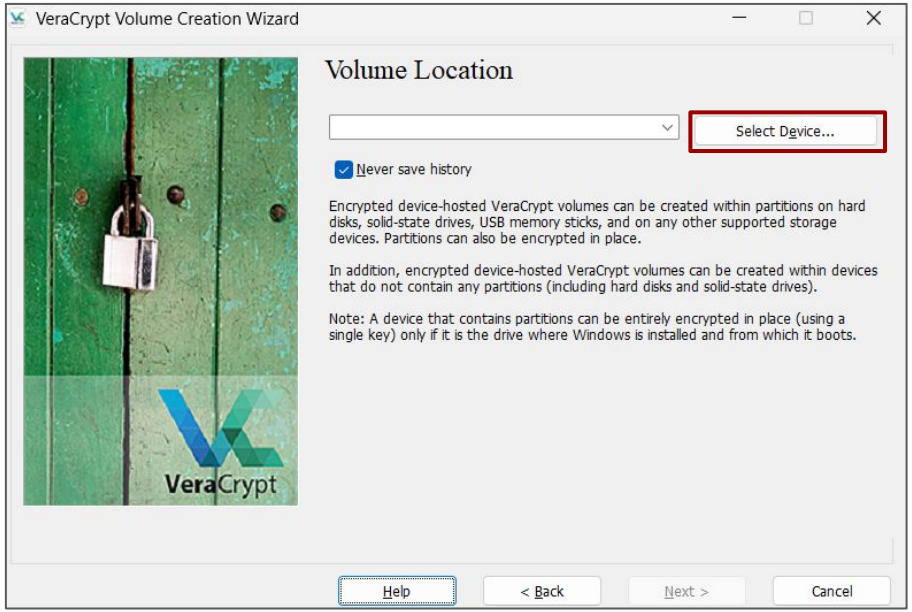
Volume Type အဆင့်ကတော့ အရှေ့က Container တွေဖန်တီးတဲ့ အဆင့်မှာရှင်းပြပေးထားပါတယ်။ Standard နဲ့ Hidden ဆိုပြီး နှစ်မျိုးရှိပါတယ်။ Veracrypt-I, Veracrypt-II Content မှာဝင်ရောက်ဖတ်ရှုနိုင်ပါတယ်။

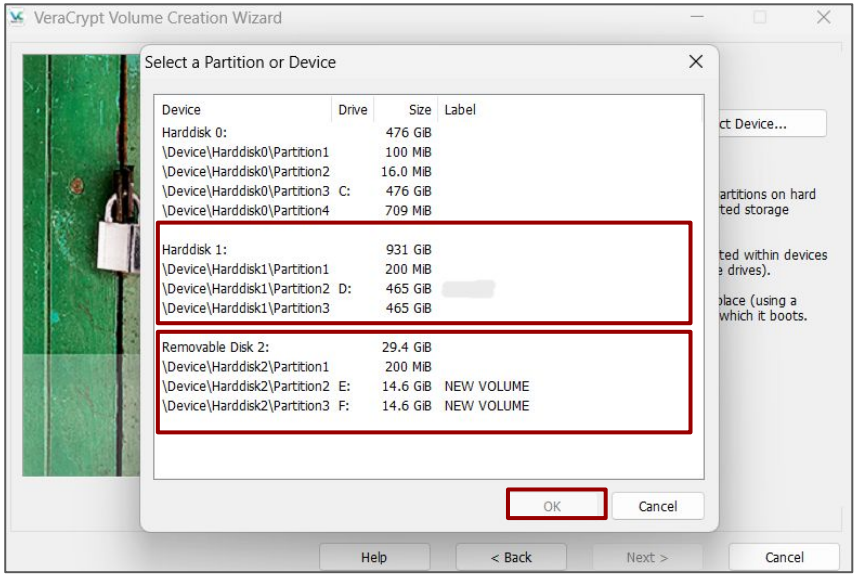


3. Standard Veracrypt Volume ကိုရွေးပါ။ Next ကိုနှိပ်ပါ။

External hard-drive or USB ကို Encrypt လုပ်ခြင်း

4. မိမိရဲ့ external hard drive or Memory Stick ရဲ့ partition ကိုရွေးချယ်ပါ။ Select Device ကိုရွေးပါ။





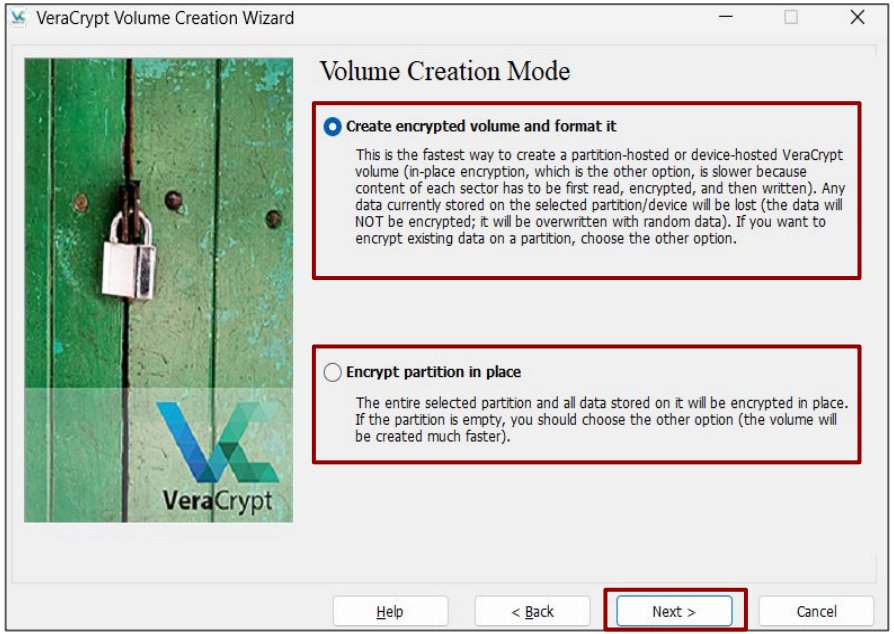
Disk နှစ်ခုရှိနေတာကို တွေ့ရမှာဖြစ်ပါတယ်။ တစ်ပိုင်းကတော့ ပုံမှန်အတိုင်းသုံးလို့ရနိုင်တဲ့ အလွတ် အပိုင်း (Partition) ဖြစ်ပါတယ်။ နောက်တစ်ပိုင်းကတော့ Veracrypt နဲ့ Encrypted လုပ်မယ့်အပိုင်းပါ။

5. မိမိကြိုက်နှစ်သက်ရာ Device ကိုရွေးပြီး OK နှိပ်ပါ။ ပြီးရင် Next နှိပ်ပါ။

External hard-drive or USB ကို Encrypt လုပ်ခြင်း

“Create encrypted volume and format it”- ဆိုတာကတော့ မိမိ Encrypt လုပ်မယ့် External Hard Drive/ Memory Stick ထဲမှာ ရှိသောဒေတာများကို Format ချပြီးမှ Encrypt လုပ်မှာဖြစ်တဲ့အတွက် အရင်တုန်းကထည့်ထားတဲ့ ဒေတာတွေ ပျက်သွားနိုင် ပါတယ်။ အရေးကြီး ဒေတာများ ဖြစ်ပါက အရင် backup လုပ်ဖို့လိုပါတယ်။

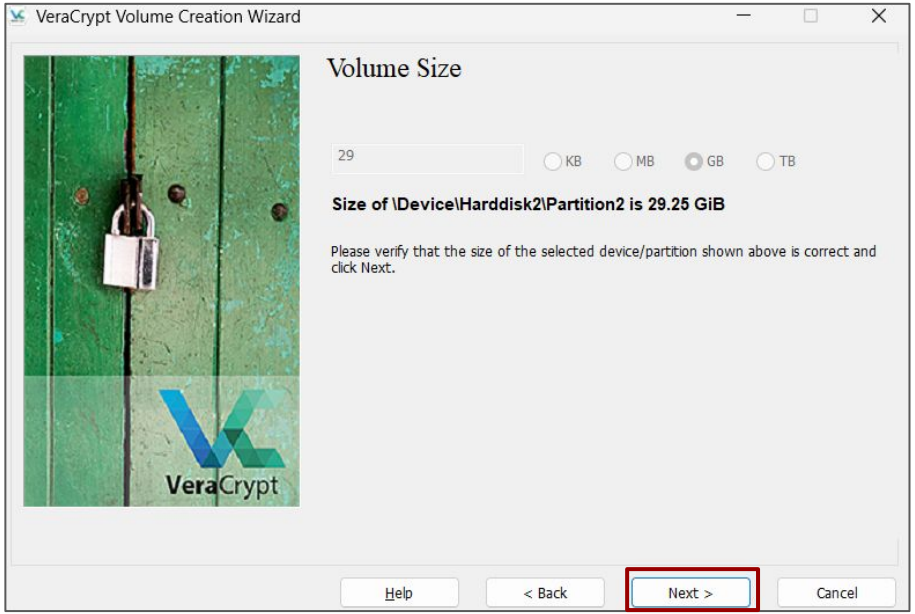
“Encrypt partition in place”- ဆိုတာကတော့ External Hard Drive/ Memory stick ထဲမှာရှိနှင့်ပြီးသား ဒေတာတွေကို မဖျက်ပဲ Encrypted လုပ်ခြင်းဖြစ်ပါသည်။ ဒေတာတွေ Backup လုပ်ဖို့အဆင်မပြေဘူး ဆိုရင် ဒီဟာကို ရွေးပါ။ ဒေတာတွေမပျက်ဘဲကျန်နေပါလိမ့်မယ်။ သို့သော် အပေါက် Option ထပ် Processing အချိန်ပိုကြာပါတယ်။ 500 GB လောက်ဆိုရင် ခန့်မှန်းချေအားဖြင့် ၆ နာရီလောက် ကြာနိုင်ပါတယ်။



6.မိမိနှင့်အဆင်ပြေတဲ့ နည်းလမ်းကိုရွေးပြီး Next ကိုနှိပ်ပါ။

External hard-drive or USB ကို Encrypt လုပ်ခြင်း

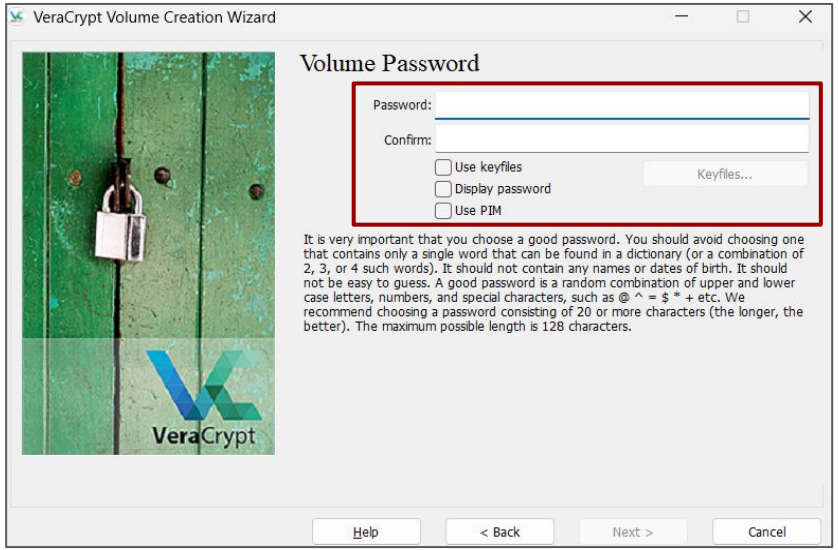
7. Encryption options ရဲ့ Encryption Algorithm မှာ AES ဒါမှမဟုတ် မိမိနှစ်သက်ရာကိုရွေးပြီး Next ကိုဆက်နှိပ်ပါ။ Volume Size အပိုင်းကတော့ ချိန်လို့ရမှာမဟုတ်ပါဘူး။ Next ပဲဆက်နှိပ်ပါ။

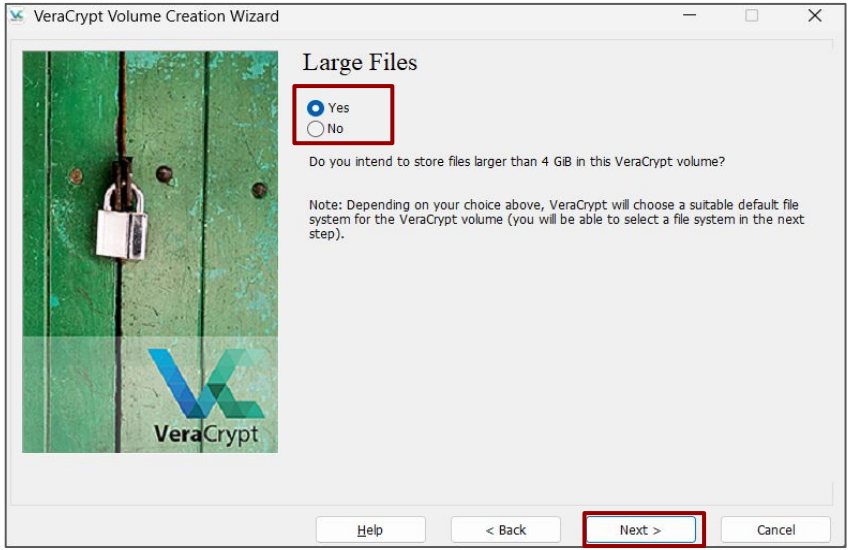


External hard-drive or USB ကို Encrypt လုပ်ခြင်း

8. ဒီနေရာက အရေးကြီးပါတယ်။ Password ကို မှတ်မိလွယ်ပီး ခိုင်မာအားကောင်းတဲ့ Password ထားပါ။ Password ကို မမေ့ပစ်ဖို့လည်းလိုပါသည်။ မေ့သွားပါက မိမိ Encrypt လုပ်ထားသော Data များကို ပြန်ပြီးရနိုင်မည်မဟုတ်ပါ။

- **Password ထားပါ။**
- **Yes ကိုနှိပ်ပါ။ 4 GB ထက်ကျော်လွန်တဲ့ data တွေကိုထည့်ဖို့ volume ကြီးကြီးတည်ဆောက်မယ်ဆိုရင် မိမိရဲ့ Hard Drive File System က သင့်လျော်သလို ပြောင်းသွားပါလိမ့်မယ်။ FAT(default) to exFAT.**





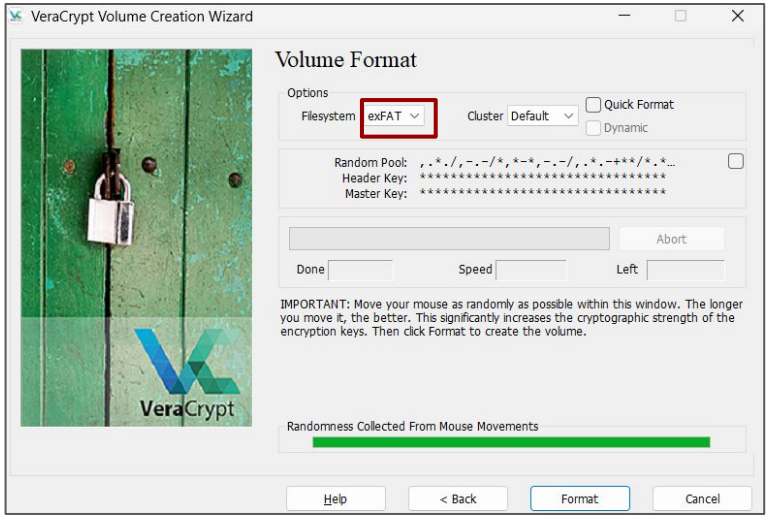
External hard-drive or USB ကို Encrypt လုပ်ခြင်း

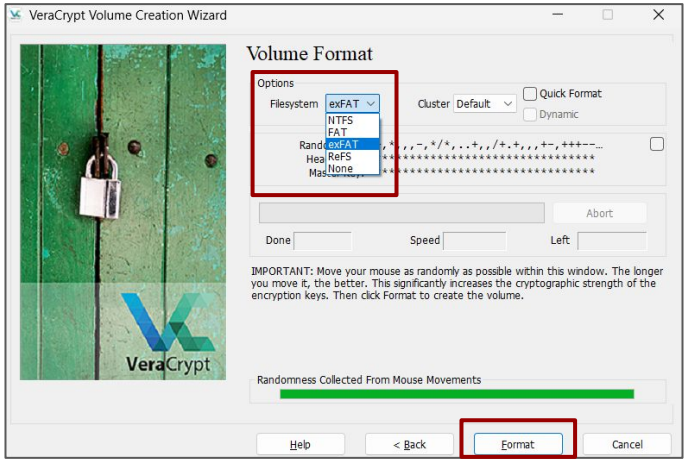
FAT - File System အဟောင်းပါ။ တစ်ဖိုင်ကို 4GB ထပ်ကျော်ပီးသိမ်းလို့မရပါဘူး။

exFAT - File System အသစ်ပါ။ ဖိုင်တစ်ဖိုင်ရဲ့ Size ကို ကန့်သတ်မထားပါဘူး။ ဘယ် Operating System မှာမဆို အသုံးပြုနိုင်ပါတယ်။

NTFS - Windows ရဲ့ သီးသန့် File System ပါ။ Partitions အတိုးအချုံ့ ကို လွယ်ကူစွာ လုပ်နိုင်ပါတယ်။ FAT and exFAT ကတော့မဆောင်ရွက်နိုင်ပါဘူး

ReFS - Windows ရဲ့ သီးသန့် File System ပါပဲ။ ဒေတာ တွေ့ပျက်စီးပျောက်ခြင်းကနေ တစ်ခြား File System များထပ် ပိုမိုကာကွယ်ပေးနိုင်ပါတယ်။ လူသုံးနည်းပါတယ်။

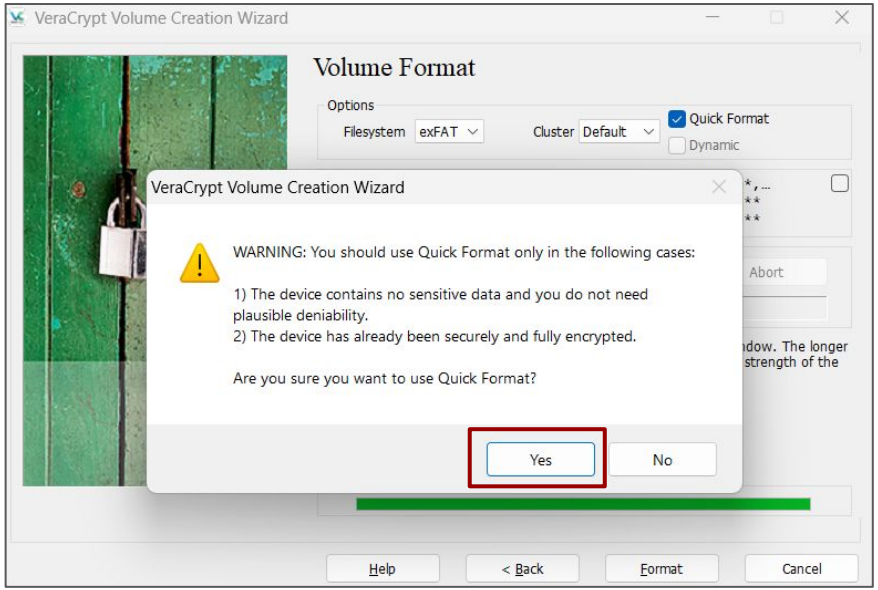




9. ကြိုက်နှစ်သက်ရာ File အမျိုးအစားရွေးပြီး Format ကိုနှိပ်ပါ။

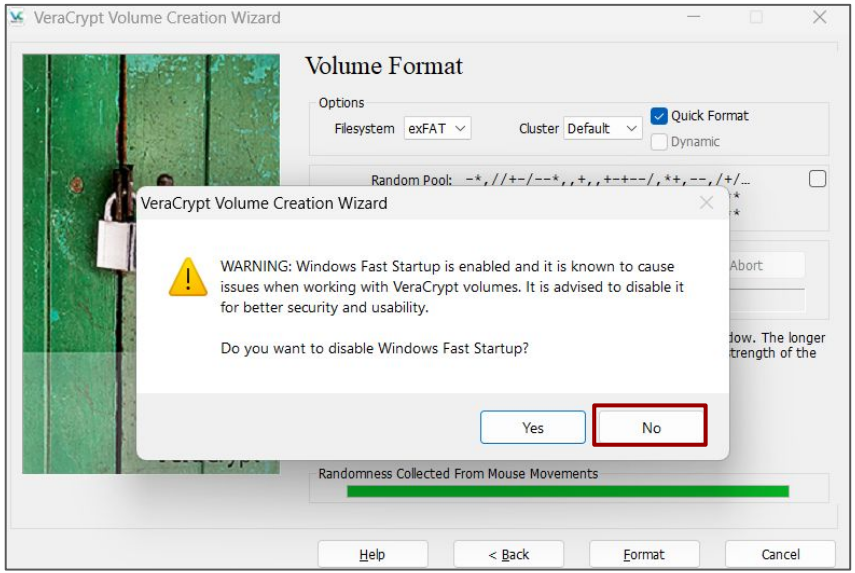
External hard-drive or USB ကို Encrypt လုပ်ခြင်း

Quick Format ကိုရွေးခဲ့ရင် Processing Time ကတော်တော် မြန်ပါတယ်။ သို့သော် Encryption မပါဝင်တော့တဲ့အတွက် Sensitive data တွေသိမ်းဖို့မသင့်တော်တော့ပါ။

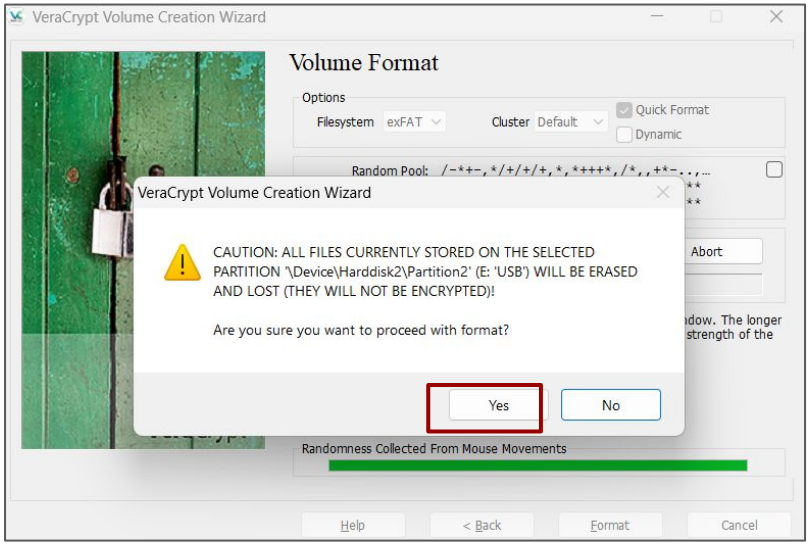


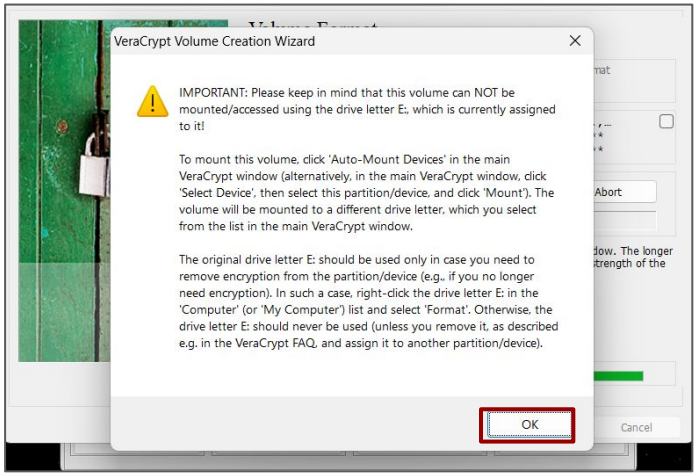
10. Quick Format ကိုရွေးချယ်လိုက်တယ်ဆိုရင်တော့ ဒီ Box လေး ပေါ်လာပါလိမ့်မယ်၊ Yes ကိုရွေးချယ်ပါ။

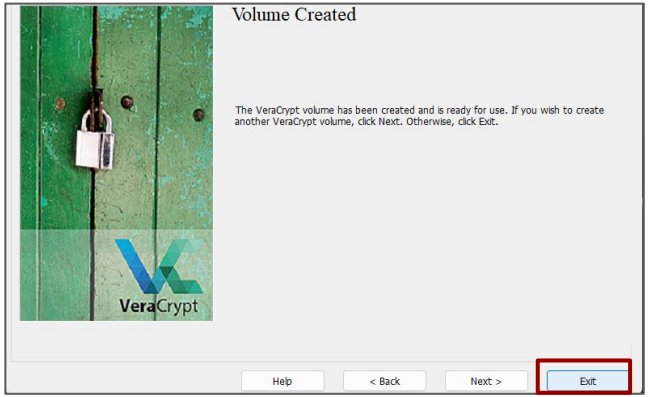
11. Windows Fast Startup ကို Disable လုပ်မလားမေးရင် No ကိုရွေးပါ။



External hard-drive or USB ကို Encrypt လုပ်ခြင်း





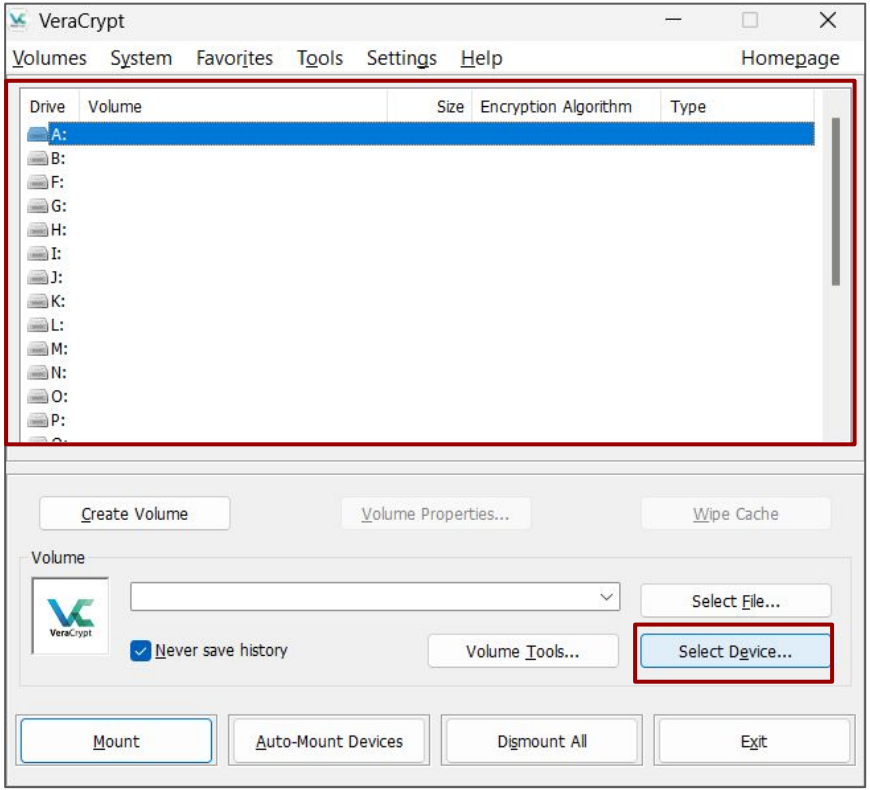


12. Yes နှိပ်ပါ။

ပြီးရင် OK နှိပ်ပါ။

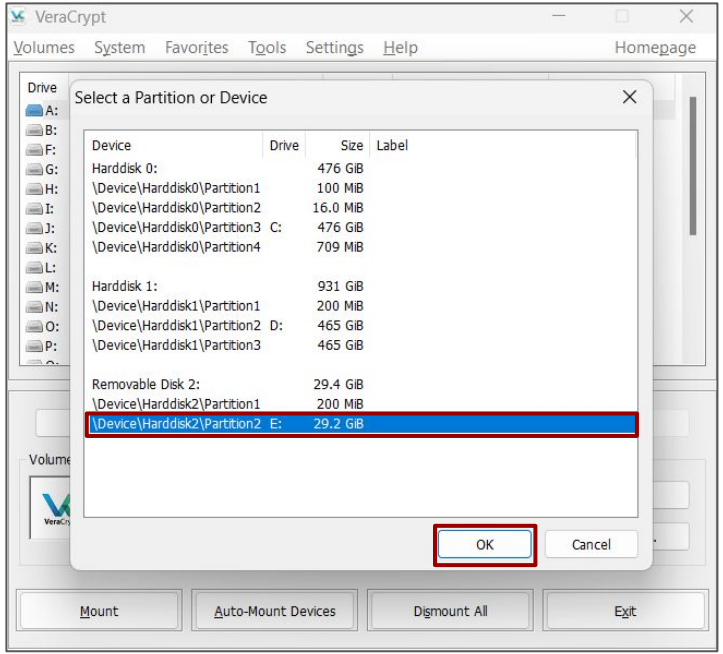
Volume ဖန်တီးပြီးပါပြီ။ Exit ကို နှိပ်ပါ။

External hard-drive or USB ကို Encrypt လုပ်ခြင်း



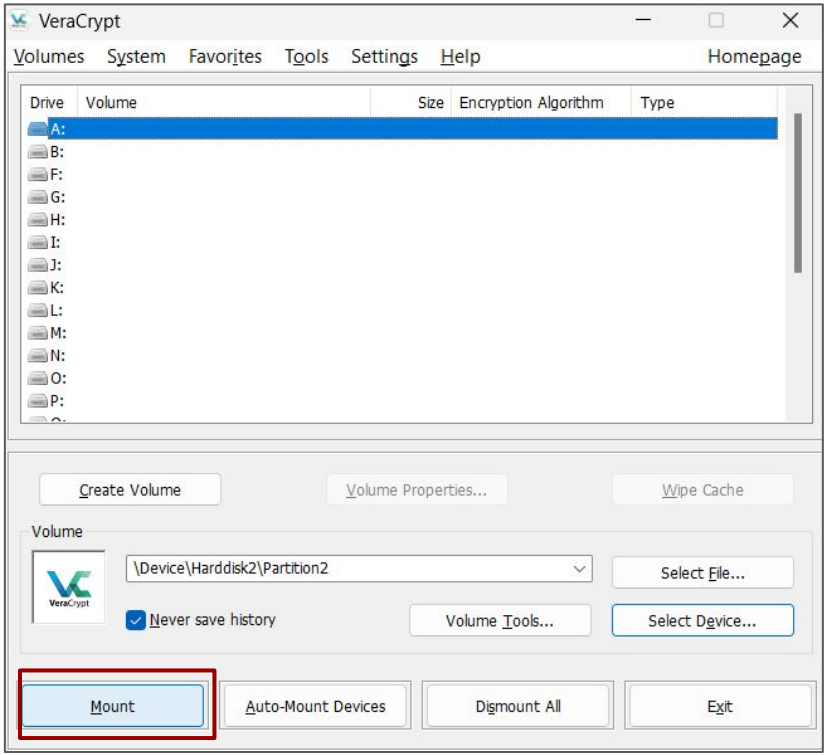
13. ပြန်ဖွင့်ဖို့ Drive letter ကိုအရင်ရွေးပီး Select Device နှိပ်ပါ။

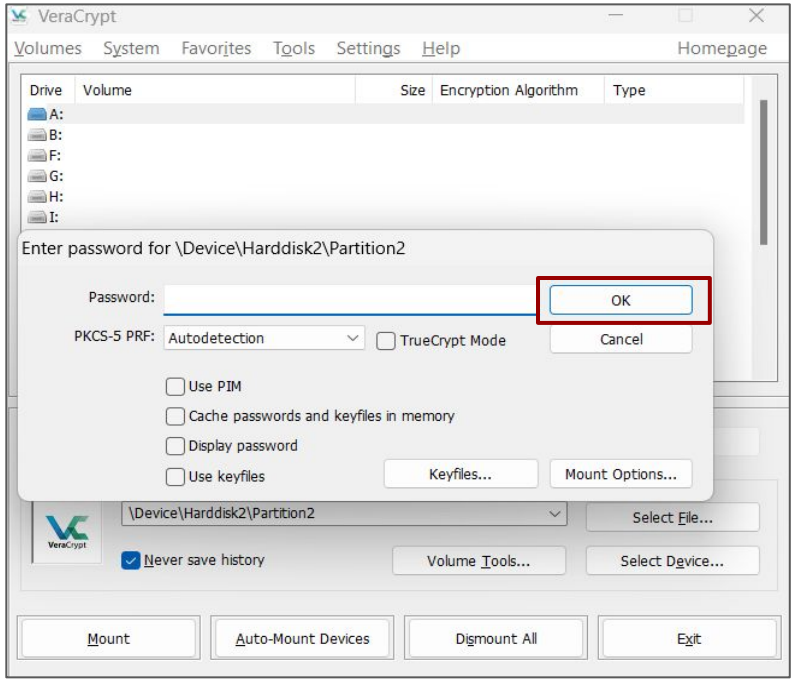
14. မိမိရဲ့ hard drive ရဲ့ encrypted partition ကိုရွေးပြီး OK နှိပ်ပါ။



External hard-drive or USB ကို Encrypt လုပ်ခြင်း

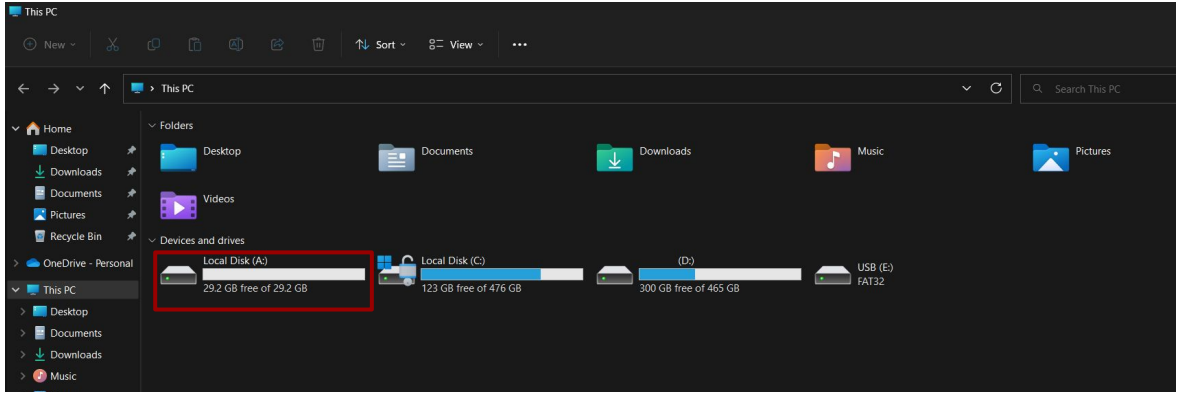
15. Mount နှိပ်ပြီး မိမိထားခဲ့သော Password ကိုရိုက်ထည့်ပေးပါ။ ပြီးရင် OK နှိပ်ပါ။





External hard-drive or USB ကို Encrypt လုပ်ခြင်း

16. ရွေးထားသော hard drive ကို နှစ်ချက်နှိပ်ပြီး ဖွင့်လို့ရသလို This PC/My Computer ထဲကနေလည်းသွားရှာလို့ရပါတယ်။



Veracrypt ဖြင့် Encrypted hard drive or USB ကိုပြန်ထိုးပြီး ဖွင့်ကြည့်ပါက Format ရိုက်မလားဆိုပြီး မေးပါတယ်။

Cancel သာနှိပ်ပါ။ Format ကိုမတော်တဆနှိပ်မိပါက Encrypt လုပ်ထားတာ နဲ့ ထည့်သိမ်းထားတဲ့ ဒေတာတွေကို ပျက်သွားနိုင်ပါတယ်။
ဒါဆိုရင်တော့ Hard Disk သို့မဟုတ် Memory Stick ကို Partition ခွဲပြီး Encrypted ပြုလုပ်ခြင်း ပြီးဆုံးသွားပြီဖြစ်ပါတယ်။