Cách mã hóa ổ đĩa hệ thống Windows với VeraCrypt

Một số thiết bị chạy Windows 10 được tích hợp sẵn "mã hóa thiết bị", nhưng số còn lại yêu cầu bạn phải trả thêm tiền để sử dụng tính năng BitLocker trên Windows Pro nhằm mã hóa toàn bộ đĩa cho lý do bảo mật. Tuy nhiên, bạn hoàn toàn có thể sử dụng phần mềm VeraCrypt miễn phí và có mã nguồn mở để mã hóa toàn bộ các ổ đĩa trên máy tính của mình với bất kỳ phiên bản Windows nào.

Nói qua một chút về ý nghĩa thì ổ cứng là nơi lưu trữ các tập tin quan trọng của bạn. Vậy thì sẽ ra sao nếu ổ đĩa gặp trục trặc hoặc tệ hơn là bị đánh cắp? Nếu bạn chưa tạo bản sao lưu thì toàn bộ dữ liệu quan trọng đó sẽ có nguy cơ cao bị thất thoát hoặc thậm chí là rơi vào tay kẻ xấu. Trong trường hợp này, mã hóa là cách tốt nhất để đảm bảo những người lạ hoặc kẻ tấn công sẽ không thể đọc được các dữ liệu trong ổ đĩa của bạn. Nó sẽ xáo trộn các tệp của bạn theo những quy luật khác nhau và bạn sẽ phải cần đến một khóa bí mật để truy cập vào các dữ liệu đã được mã hóa. Thế nên ngay cả khi ai đó có quyền truy cập vào ổ đĩa cứng vật lý của bạn, họ buộc phải có thêm mật khẩu (hoặc tệp khóa - keyfile) thì mới có thể thực sự thấy được những gì bạn lưu trữ trên ổ đĩa.

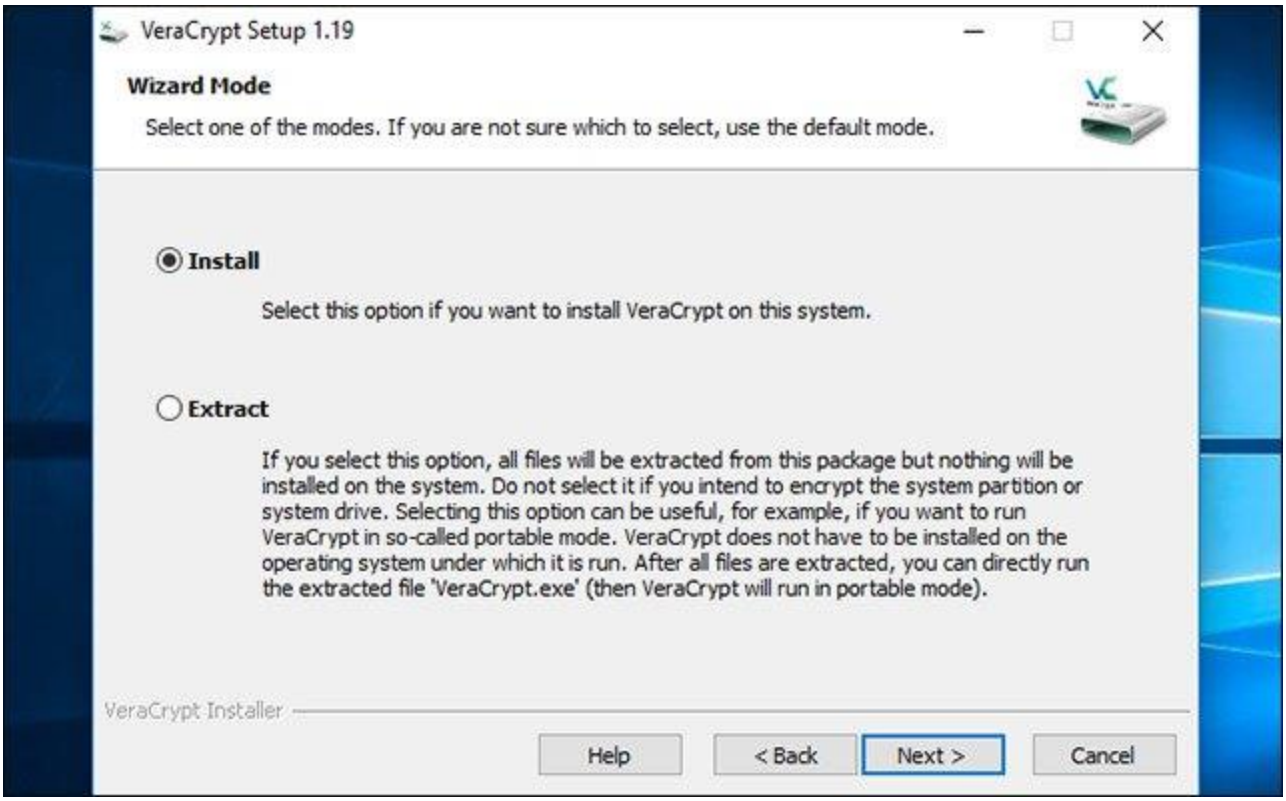
VeraCrypt là một công cụ bảo mật miễn phí và có mã nguồn mở mà bạn có thể sử dụng để thiết lập mã hóa cho toàn bộ các ổ đĩa trên bất kỳ máy tính Windows nào. Phần mềm này hoạt động tốt trên Windows 10, 8, 7, Vista và thậm chí là cả XP.

Sử dụng VeraCrypt không hề phức tạp như nhiều người vẫn nghĩ: Sau khi thiết lập thành công, bạn chỉ cần nhập đúng mật khẩu mã hóa mỗi khi khởi động máy tính và sử dụng máy tính như bình thường sau khi khởi động. VeraCrypt xử lý mã hóa trong nền và mọi thứ khác đều diễn ra một cách minh bạch. Ngoài ra, nó cũng có thể tạo vùng chứa tệp được mã hóa, nhưng ở đây chúng ta sẽ chỉ tập trung vào việc làm thế nào để mã hóa ổ đĩa hệ thống của bạn mà thôi.

VeraCrypt là một dự án dựa trên mã nguồn của phần mềm TrueCrypt cũ, vốn đã ngừng hoạt động. VeraCrypt có nhiều bản sửa lỗi và hỗ trợ các PC hiện đại với phân vùng hệ thống EFI, cấu hình mà nhiều máy tính Windows 10 sử dụng.

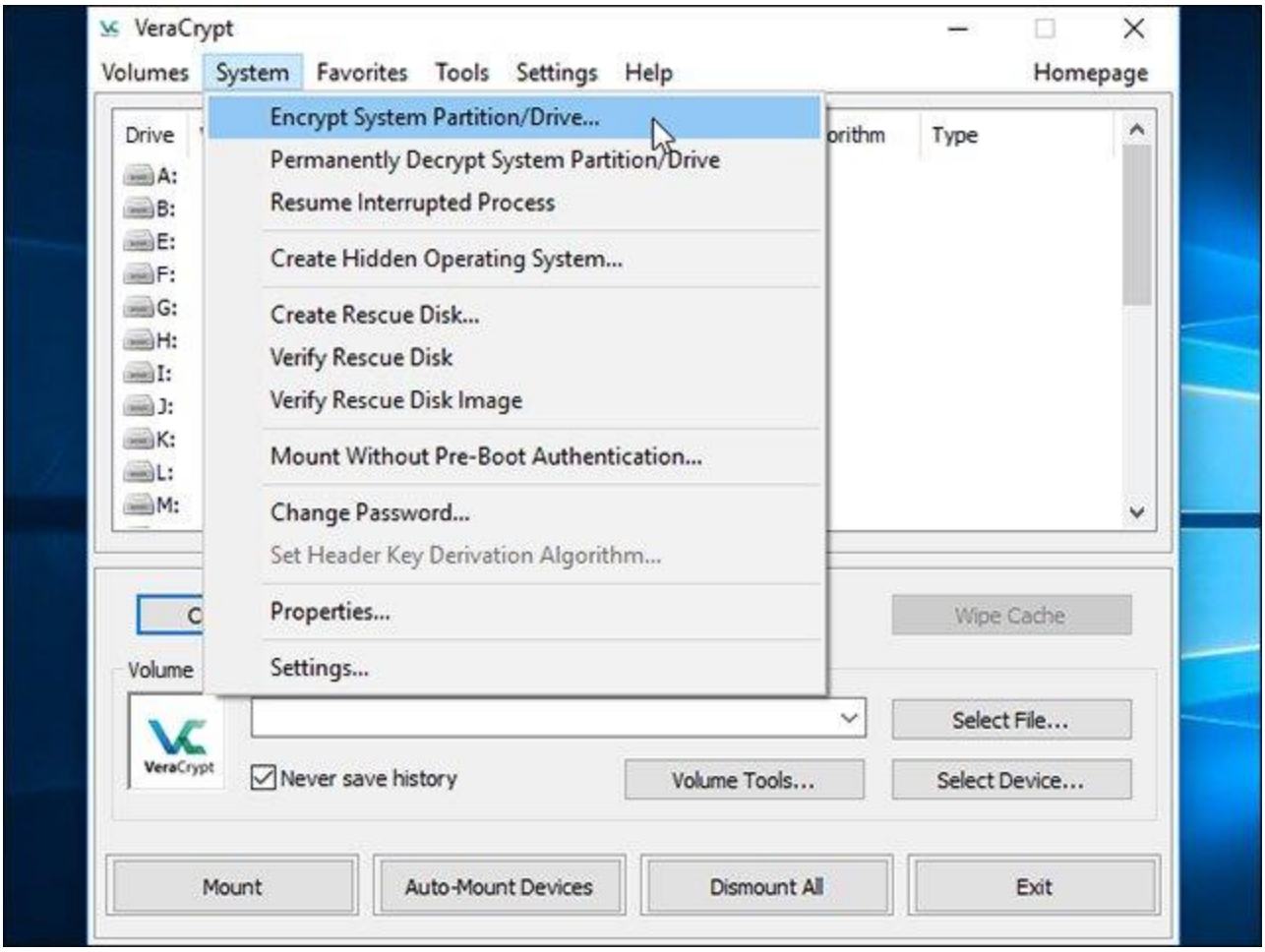
Làm thế nào để cài đặt VeraCrypt và mã hóa ổ đĩa hệ thống?

Tất nhiên rồi, đầu tiên bạn sẽ cần phải tải VeraCrypt về máy, chạy trình cài đặt và chọn tùy chọn **Install**. Bạn có thể giữ lại tất cả các thiết lập mặc định trong trình cài đặt chỉ cần nhấp vào đồng ý với các điều khoản (next) cho đến khi VeraCrypt bắt đầu cài đặt trên máy tính của bạn.



Sau khi VeraCrypt được cài đặt, hãy mở menu Start của bạn và khởi động shortcut VeraCrypt.

Nhấn vào **System> Encrypt System Partition/Drive** trong cửa sổ VeraCrypt để bắt đầu thiết lập mã hóa cho ổ đĩa.



Bạn sẽ được hỏi xem có muốn sử dụng mã hóa hệ thống **Normal** (bình thường) hoặc **Hidden** (ẩn) hay không.

Tùy chọn **Normal** sẽ mã hóa phân vùng hệ thống hoặc các trình điều khiển một cách bình thường. Khi bạn khởi động máy tính, bạn sẽ phải nhập mật khẩu mã hóa để truy cập vào hệ thống. Không ai có thể truy cập được vào hệ thống các tệp của bạn nếu như không nắm được mật khẩu.

Tùy chọn **Hidden** sẽ tạo ra một hệ điều hành trong một khối VeraCrypt ẩn. Lúc này, bạn sẽ có cả hệ điều hành "thực" (đã bị ẩn đi) và hệ điều hành "mồi nhử" do VeraCrypt tạo ra. Khi bạn khởi động máy tính, bạn có thể nhập mật khẩu thực để khởi động hệ điều hành ẩn hoặc mật khẩu bình thường để khởi động và truy cập vào hệ điều hành mồi nhử. Vậy thì tùy chọn Hidden này để phục vụ cho những tình huống như thế nào? Nếu ai đó buộc bạn phải cung cấp cho họ quyền truy cập vào ổ đĩa đã mã hóa của mình, ví dụ như tống tiền chẳng hạn, bạn có thể cung cấp cho họ

mật khẩu của hệ điều hành mồi và họ sẽ không thể biết rằng hệ điều hành thực đang bị ẩn đi.

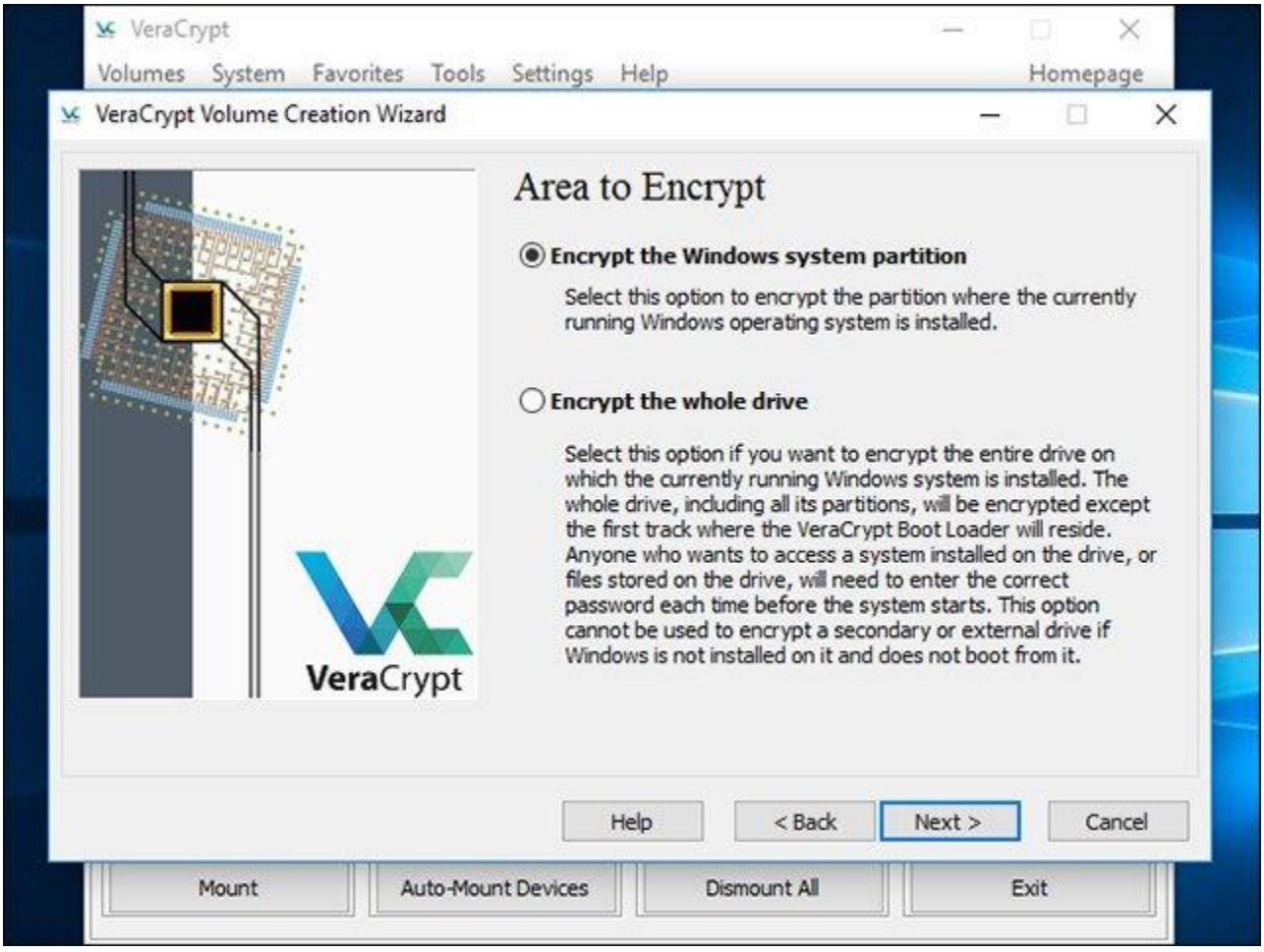
Về mặt mã hóa mà nói thì việc sử dụng mã hóa bình thường vẫn sẽ có thể giữ an toàn tuyệt đối cho các dữ liệu của bạn. Tùy chọn ẩn chỉ thực sự hữu ích khi bạn bị buộc phải tiết lộ mật khẩu của mình cho ai đó và bạn muốn từ chối một cách hợp lý về sự tồn tại của một hoặc một vài tập tin nào đó trong hệ thống của mình.

Nếu bạn không chắc chắn về việc mình nên dùng tùy chọn nào, tốt nhất là hãy chọn **Normal** và nhấn tiếp tục (next). Tiếp theo, chúng ta sẽ trải qua quá trình tạo phân vùng hệ thống được mã hóa bình thường, đây cũng là một trong những giai đoạn cực kỳ quan trọng trong cả quá trình. Ngoài ra, bạn cũng có thể tham khảo một số tài liệu của VeraCrypt để biết thêm thông tin về các hệ điều hành ẩn.

Bạn có thể chọn **Encrypt the Windows system partition** (mã hóa phân vùng hệ thống Windows) hoặc **Encrypt the whole drive** (mã hóa toàn bộ ổ đĩa), tùy thuộc vào sở thích cá nhân!

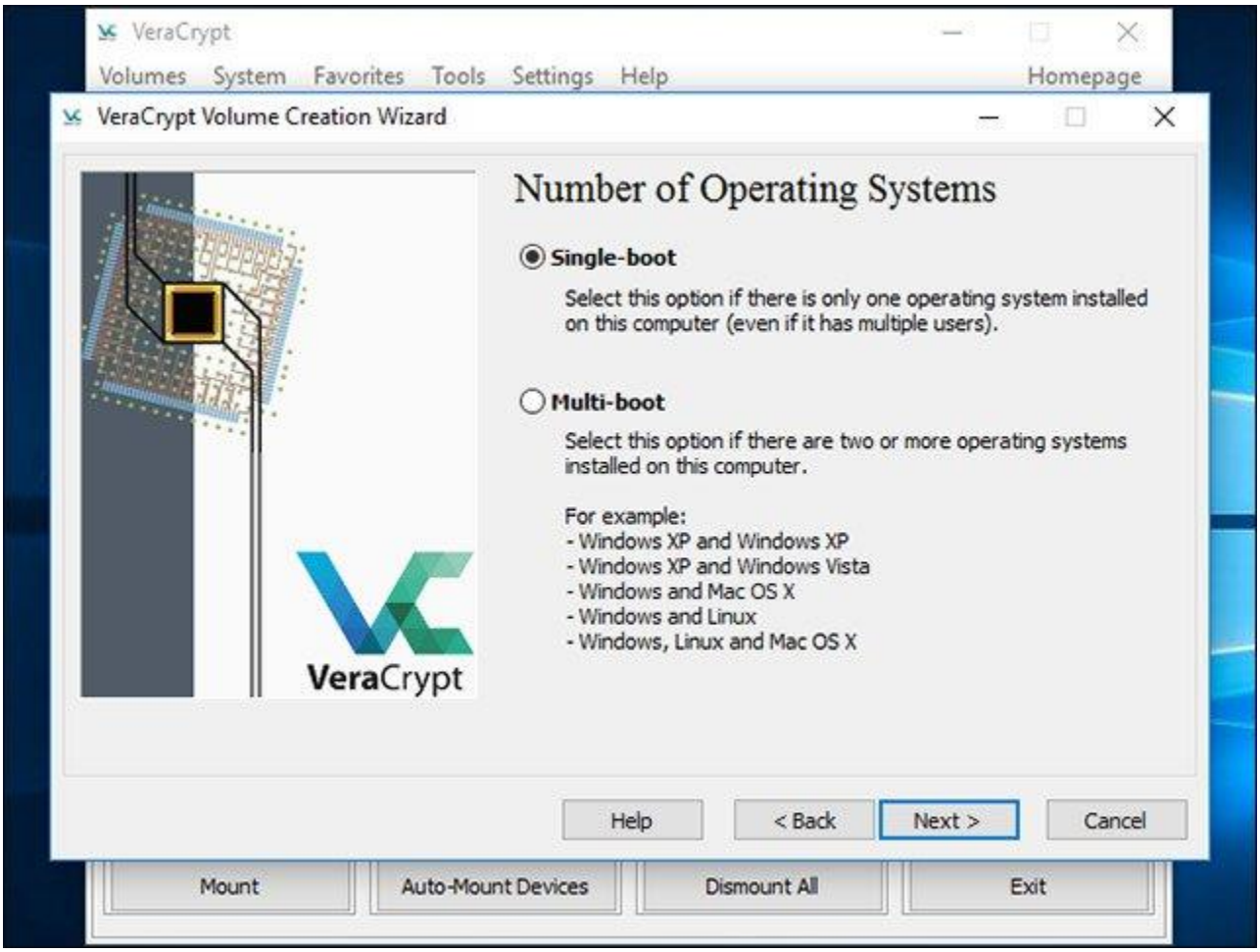
Nếu phân vùng hệ thống Windows là phân vùng duy nhất trên ổ đĩa của bạn, các tùy chọn về cơ bản sẽ giống nhau. Còn nếu hệ thống của bạn có nhiều phân vùng khác nhau và bạn chỉ muốn mã hóa cho phân vùng hệ thống Windows, hãy chọn **Encrypt the Windows system partition.**

Trong trường hợp bạn có nhiều phân vùng với những dữ liệu nhạy cảm, ví dụ như phân vùng hệ thống tại ổ C: và phân vùng tệp tại ổ D:... hãy chọn **Encrypt the whole drive** để đảm bảo rằng tất cả các phân vùng Windows của bạn đều sẽ được mã hóa.

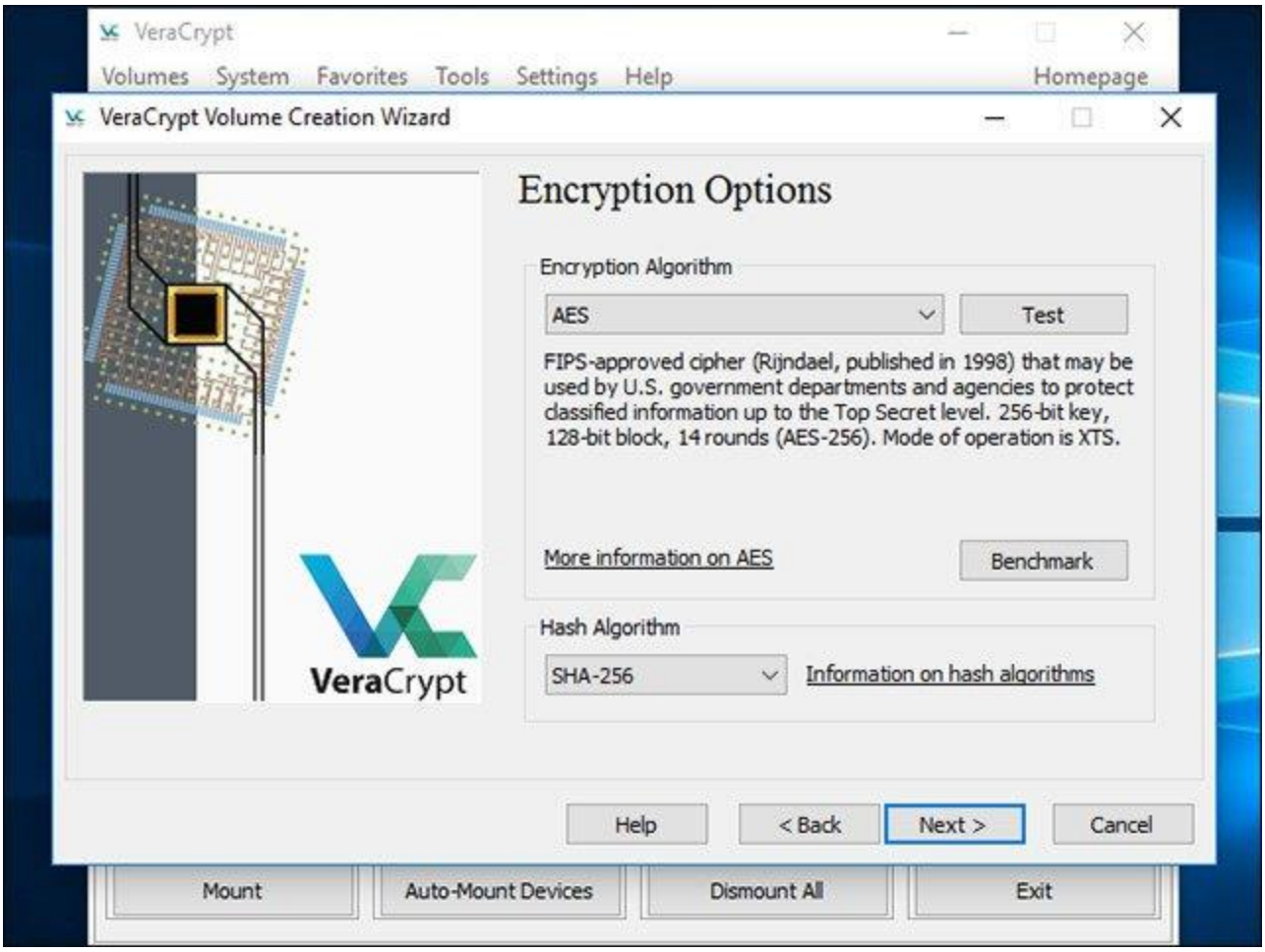


VeraCrypt sẽ hỏi bạn rằng có bao nhiêu hệ điều hành đang chạy trên máy tính của bạn. Hầu hết mọi người sẽ chỉ có một hệ điều hành được cài đặt trên hệ thống và

trong trường hợp này họ sẽ chọn **Single-boot**. Nếu bạn có nhiều hơn một hệ điều hành được cài đặt và có thể lựa chọn qua lại giữa các hệ điều hành này khi khởi động máy tính thì hãy nhấn vào **Multi-boot**.



Sau đó, bạn sẽ được yêu cầu chọn phương thức mã hóa mà bạn muốn sử dụng. Mặc dù sẽ có nhiều tùy chọn khác nhau, nhưng nếu bạn không phải là người có kiến thức thực sự chuyên sâu về mã hóa dữ liệu, tốt nhất là bạn nên gắn bó với cài đặt mặc định. Trong trường hợp này, mã hóa mặc định sẽ là **AES**. Mã hóa AES và thuật toán băm SHA-256 có thể nói là một sự lựa chọn không tồi.



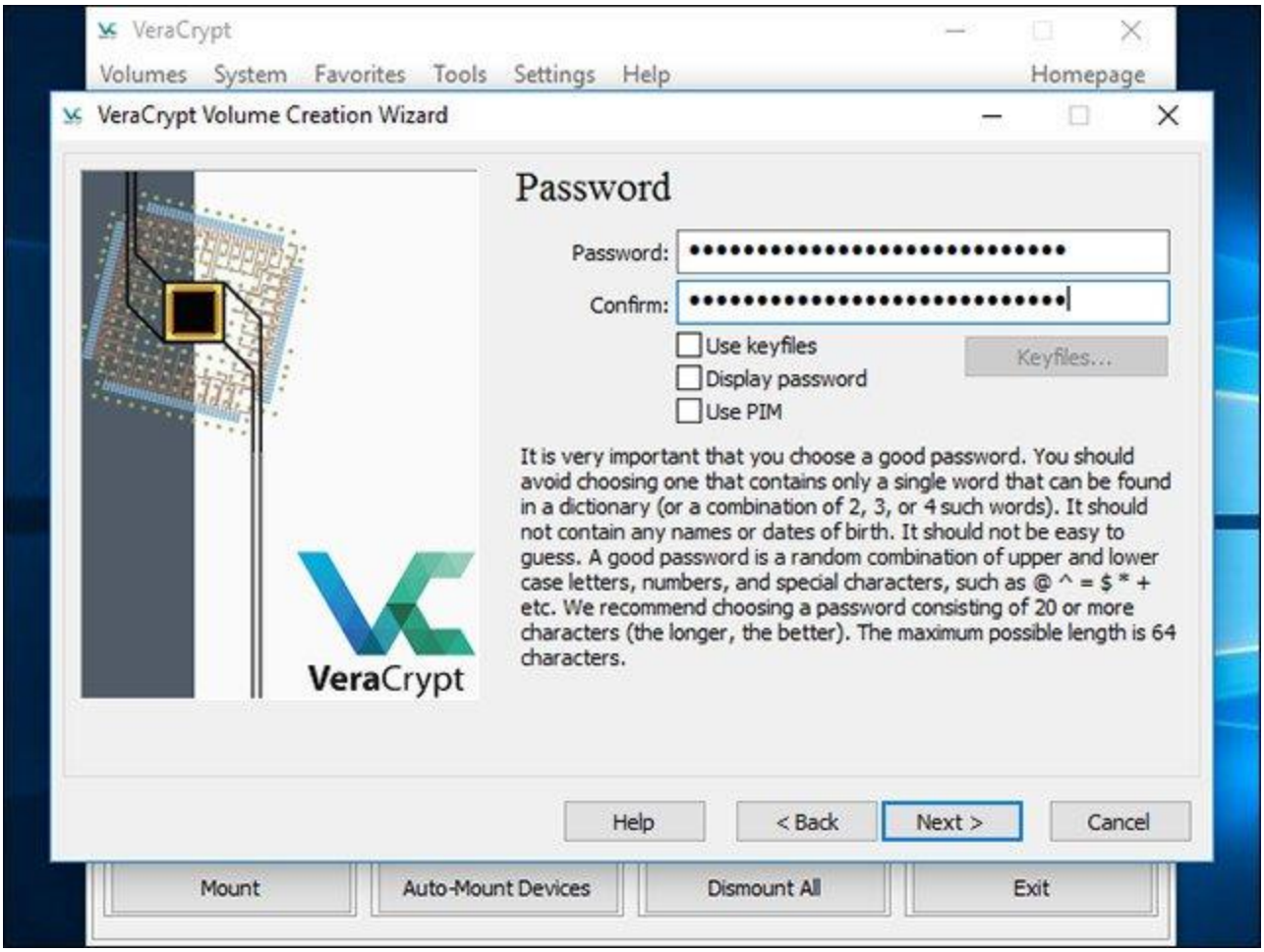
Sau đó, bạn sẽ được yêu cầu nhập mật khẩu. Theo ghi chú của VeraCrypt, việc chọn một mật khẩu tốt cũng là một yếu tố đặc biệt quan trọng mà bạn sẽ phải lưu ý. Chọn một mật khẩu rõ ràng, quen thuộc hoặc quá đơn giản sẽ khiến cho cho mã hóa của bạn dễ dàng bị tấn công brute-force.

Trình hướng dẫn khuyên bạn nên chọn một mật khẩu có ít nhất trên 20 ký tự. Bạn có thể nhập mật khẩu có tối đa 64 ký tự. Một mật khẩu lý tưởng là sự kết hợp ngẫu nhiên của các loại ký tự khác nhau, bao gồm cả chữ hoa và chữ thường, cũng như số và ký hiệu. Lưu ý là bạn sẽ mất quyền truy cập vào các tệp của mình nếu như bạn làm mất mật khẩu, do đó, đặt một mật khẩu đủ mạnh đã là quan trọng rồi, nhưng làm thế nào để đảm bảo bạn nhớ kĩ mật khẩu đó còn quan trọng hơn.

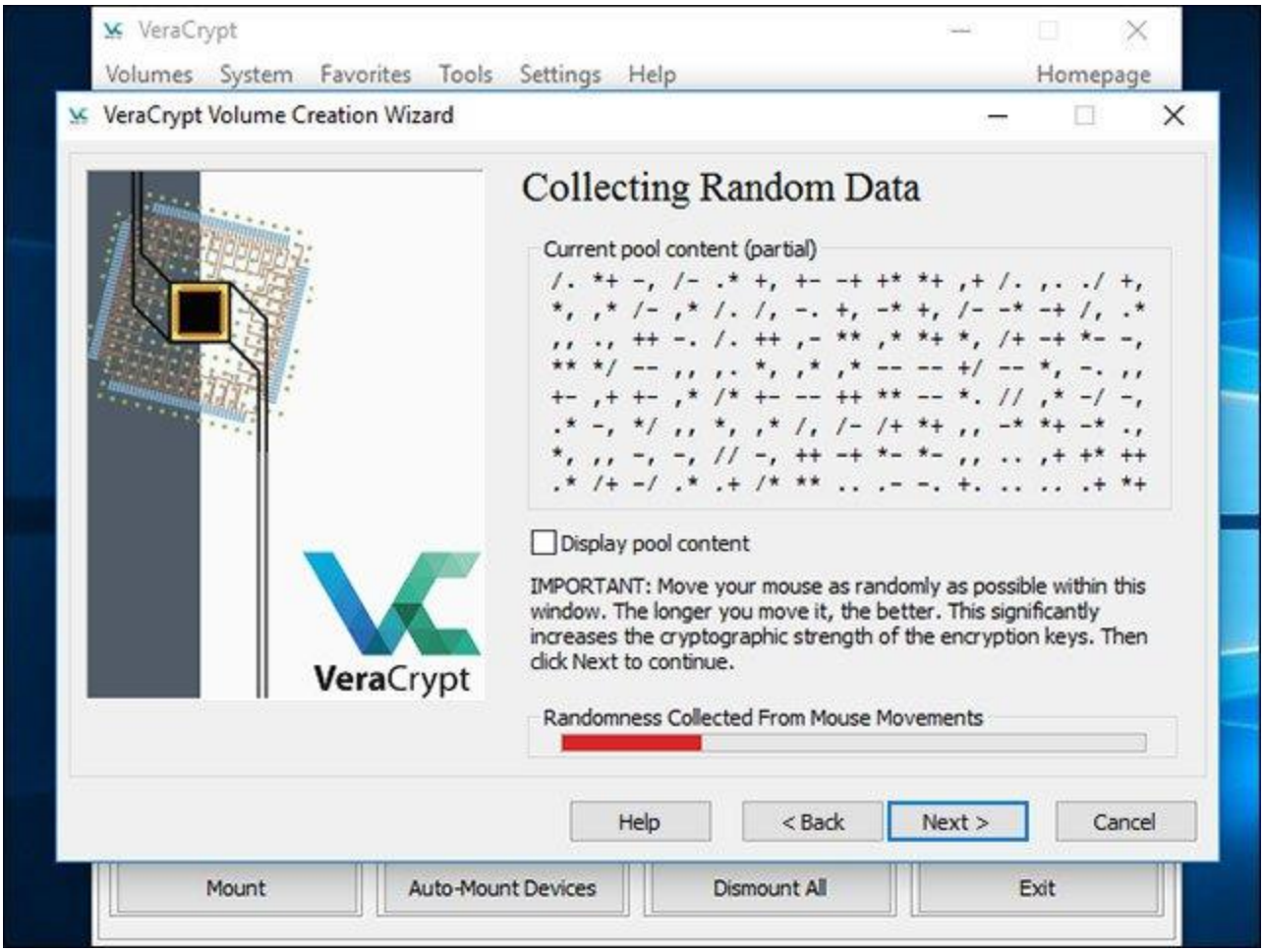
Có một vài tùy chọn về thiết lập mật khẩu khác ở đây, nhưng chúng không quá cần thiết. Đây chỉ là các tùy chọn để bạn tham khảo, nếu thấy không cần thiết phải sử dụng thì bạn cũng không nhất thiết phải áp dụng các tùy chọn này:

- Sử dụng các keyfile: Bạn có thể chọn kích hoạt Use keyfiles và cung cấp một số tệp cần thiết. Ví dụ: trên ổ USB khi bạn mở khóa ổ đĩa của mình. Nếu bạn để mất các keyfile, bạn sẽ mất quyền truy cập vào ổ đĩa của mình.
- Hiển thị mật khẩu: Tùy chọn này sẽ cho phép chỉ hiển thị đối với các trường mật khẩu trong cửa sổ này, qua đó giúp bạn xác nhận rằng nội dung bạn đã nhập là chính xác.
- Sử dụng PIM (Privileged Identity Management - Giải pháp quản lý mật khẩu đặc quyền): VeraCrypt cho phép bạn thiết lập “Personal Iterations Multiplier” (Hệ số lặp cá nhân) bằng cách kích hoạt tùy chọn Use PIM. Giá trị cao hơn có thể giúp ngăn chặn các cuộc tấn công hiệu quả hơn. Bạn cũng sẽ cần phải nhớ các số mà mình đã nhập và nhập số đó cùng với mật khẩu, do đó bạn sẽ có thêm một số thông tin khác cần phải nhớ ngoài mật khẩu của mình.

Có thể chọn bất kỳ tùy chọn nào trong số các tùy chọn trên nếu bạn muốn và sau đó nhấp vào **Next**.

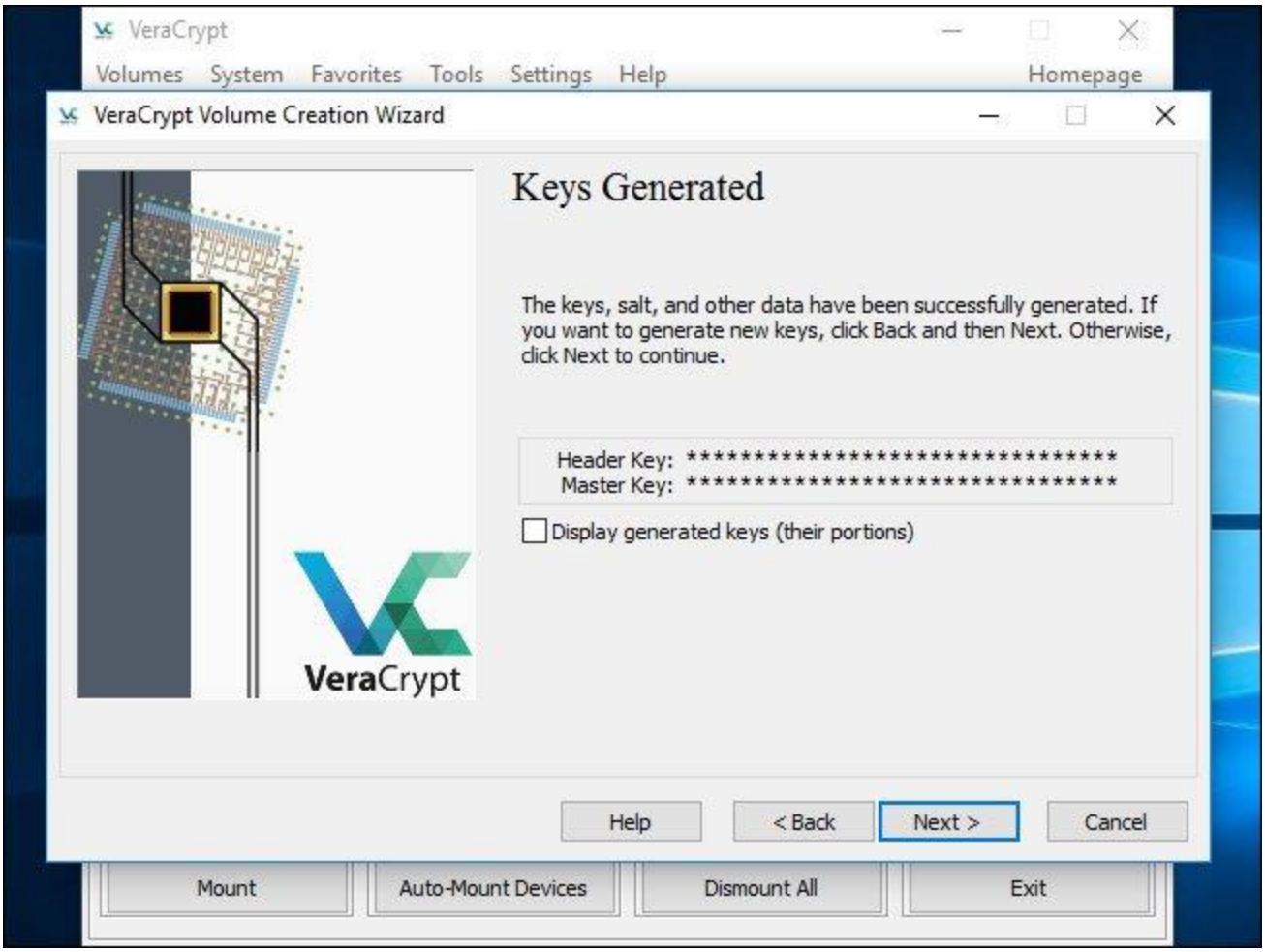


VeraCrypt sẽ yêu cầu bạn di chuyển chuột ngẫu nhiên trong phạm vi bên trong cửa sổ. Nó sẽ sử dụng các chuyển động chuột ngẫu nhiên này để tăng thêm sức mạnh cho các khóa mã hóa của bạn. Khi đã thực hiện đủ yêu cầu, hãy nhấp vào **Next**.



Tiếp theo, trình hướng dẫn sẽ thông báo cho bạn rằng nó đã tạo ra các khóa mã hóa và các dữ liệu cần thiết khác. Nhấn **Next** để chuyển sang phần tiếp theo.

Trình hướng dẫn sử dụng VeraCrypt sẽ yêu cầu bạn tạo một hình ảnh **Rescue Disk VeraCrypt** trước khi chuyển sang mục kế tiếp.



Nếu bộ bootloader hoặc dữ liệu khác của bạn bị hỏng, bạn sẽ phải khởi động lại hệ thống từ đĩa cứu hộ (Rescue Disk) nếu muốn giải mã và truy cập vào các tệp của mình. Rescue Disk cũng sẽ lưu giữ một hình ảnh sao lưu những nội dung ban đầu của ổ đĩa, cho phép bạn khôi phục lại khi cần thiết.

Lưu ý rằng bạn vẫn sẽ cần phải cung cấp mật khẩu của mình khi sử dụng Rescue Disk, vì vậy đây sẽ không phải là "chìa khóa vàng" cho phép truy cập tất cả các tệp của mình. VeraCrypt sẽ chỉ tạo một ảnh Rescue Disk ISO tại địa chỉ **C:\Users\NAME\Documents\VeraCrypt Rescue Disk.iso** theo mặc định. Bạn sẽ cần phải tự ghi hình ảnh ISO vào đĩa.

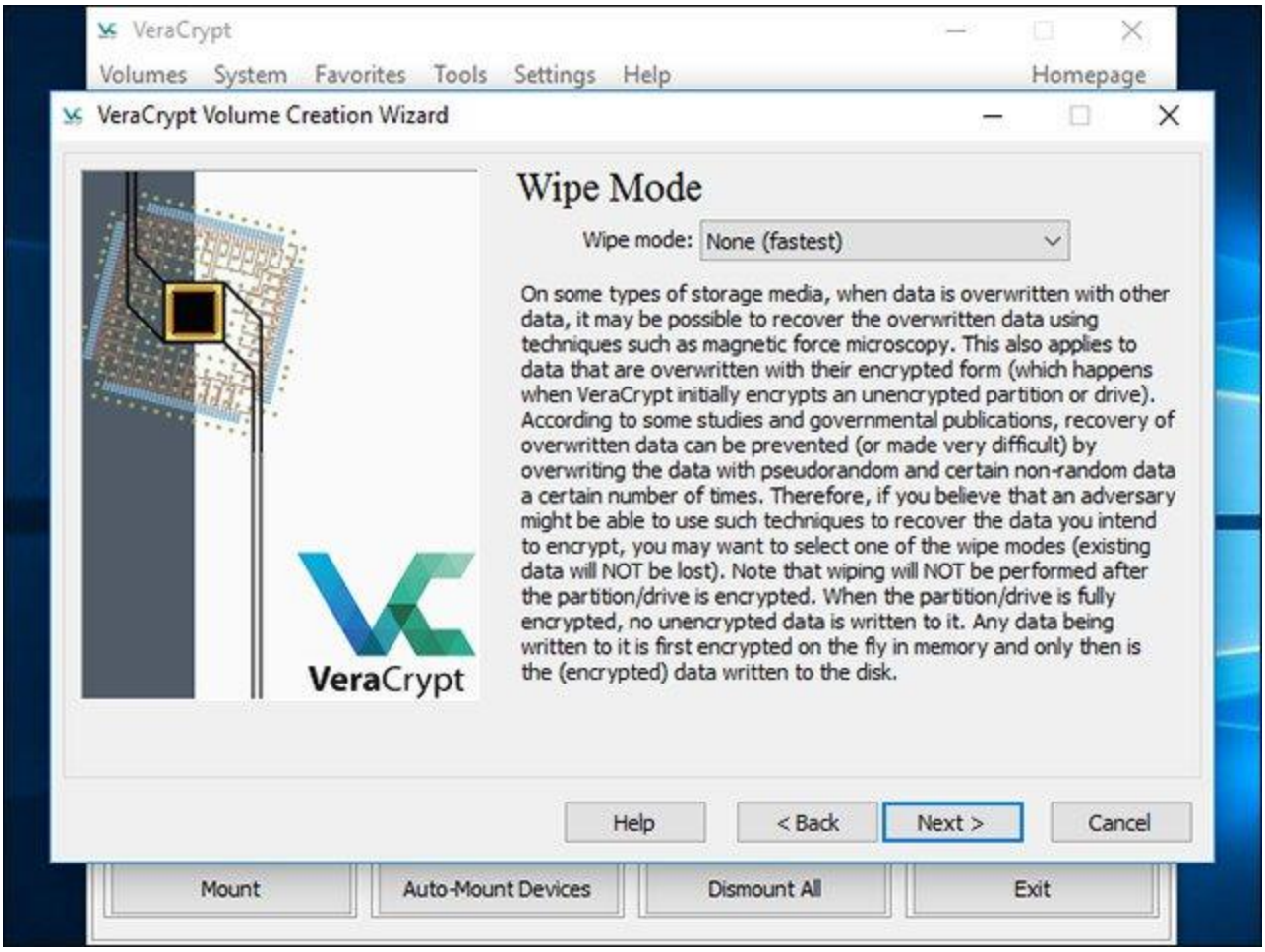
Hãy đảm bảo bạn đã ghi một bản sao của Rescue Disk để có thể truy cập vào các tệp của mình nếu có sự cố. Bạn sẽ không thể tái sử dụng cùng một Rescue Disk VeraCrypt trên nhiều máy tính mà phải cần một đĩa cứu hộ duy nhất cho mỗi PC!

Tiếp theo, bạn sẽ được yêu cầu chọn chế độ xóa mà bạn muốn sử dụng.

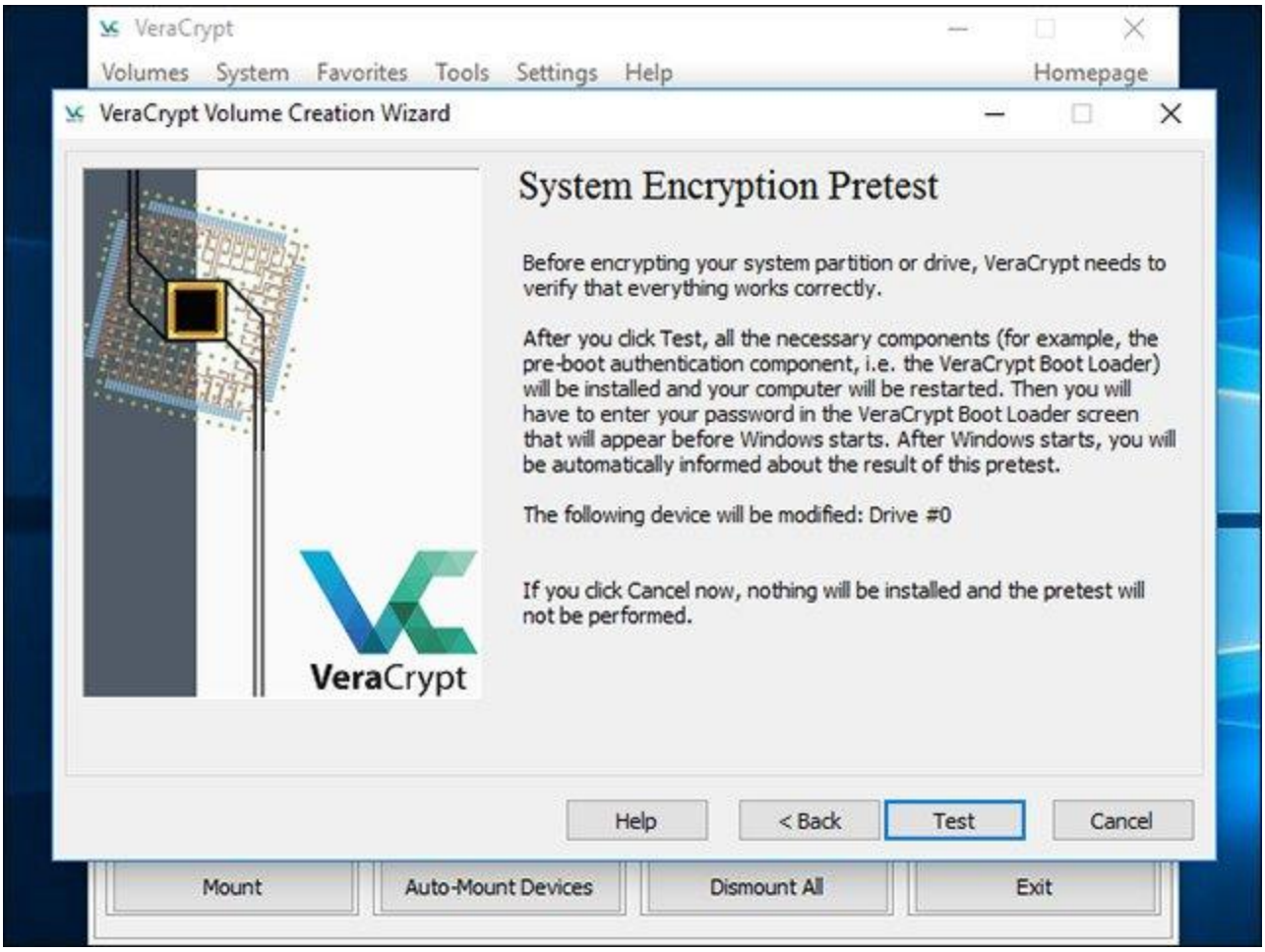
Nếu bạn có các dữ liệu nhạy cảm trên ổ đĩa và lo ngại về việc ai đó có thể kiểm tra ổ đĩa và khôi phục lại các dữ liệu đó, bạn nên chọn ít nhất **1-pass (random data)** để ghi đè các dữ liệu không được mã hóa của mình lên dữ liệu ngẫu nhiên, khiến cho các dữ liệu này khó có thể được phục hồi.

Còn nếu bạn không quan tâm đến điều này, hãy chọn **None (fastest)**. Tùy chọn này giúp xóa ổ đĩa nhanh hơn. Số lần xóa càng lớn, quá trình mã hóa sẽ càng dài.

Cài đặt này chỉ áp dụng cho quy trình thiết lập ban đầu. Sau khi ổ đĩa của bạn đã được mã hóa, VeraCrypt sẽ không cần phải ghi đè lên bất kỳ dữ liệu được mã hóa nào để bảo vệ chống lại việc khôi phục dữ liệu nữa.



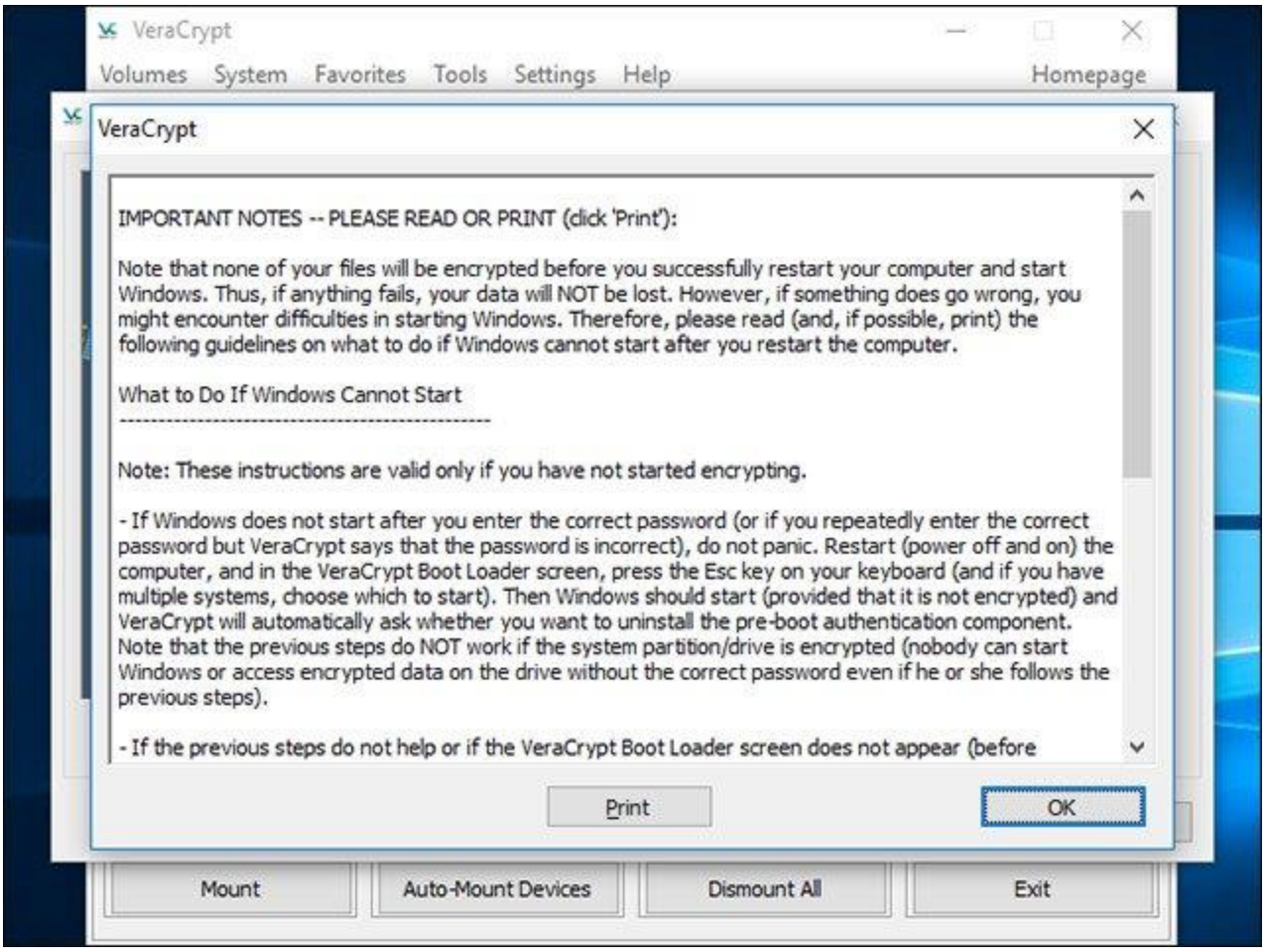
Bây giờ, VeraCrypt sẽ xác minh xem mọi thứ có đang hoạt động chính xác hay chưa trước khi nó tiến hành mã hóa ổ đĩa của bạn. Nhấp vào Test và VeraCrypt sẽ cài đặt bootloader trên PC của bạn và sau đó sẽ khởi động lại. Bạn sẽ phải nhập mật khẩu mã hóa khi nó khởi động.



VeraCrypt sẽ cung cấp thông tin về những việc bạn cần làm nếu Windows không thể tự khởi động. Nếu Windows không khởi động đúng cách, bạn nên khởi động lại PC và tại màn hình bootloader của VeraCrypt, hãy nhấn phím **Esc** trên bàn phím. Windows sẽ bắt đầu và hỏi xem bạn có muốn gỡ cài đặt bootloader của VeraCrypt hay không.

Nếu cách này không hiệu quả, bạn nên lắp đĩa cứu hộ VeraCrypt vào PC và khởi động từ đĩa này. Chọn tùy chọn sửa **Repair Options > Restore Original System Loader** trong giao diện của Rescue Disk. Sau đó khởi động lại PC của mình.

Bấm **OK** và sau đó bấm **Yes** để khởi động lại PC của bạn.



Bạn sẽ phải nhập mật khẩu mã hóa VeraCrypt khi PC khởi động. Nếu bạn không sử dụng số PIM tùy chỉnh, chỉ cần nhấn Enter tại hộp thoại nhắc PIM để chấp nhận giá trị mặc định.

Đăng nhập vào máy tính của bạn khi màn hình chào mừng thông thường xuất hiện. Bạn sẽ thấy sự xuất hiện của cửa sổ Pretest Completed.

VeraCrypt cũng khuyên bạn nên sao lưu cả các tệp đang được mã hóa bởi nếu hệ thống bị ngắt điện hoặc bị treo, một số tệp của bạn sẽ bị hỏng và không thể phục hồi, do đó, việc sao lưu các tệp quan trọng, đặc biệt khi mã hóa ổ đĩa hệ thống cũng là một lưu ý hết sức quan trọng. Nếu bạn cần sao lưu các tệp của mình, hãy nhấp vào nút **Defer** và sao lưu các tệp. Sau đó bạn có thể khởi chạy lại VeraCrypt và bấm vào **System> Resume Interrupted Process** để tiếp tục quá trình mã hóa.

Nhấp vào nút **Encrypt** để quá trình mã hóa ổ đĩa hệ thống của PC thực sự được bắt đầu.

Trước tiên, VeraCrypt sẽ cung cấp thông tin về thời điểm bạn nên sử dụng Rescue Disk. Sau đó, nó sẽ bắt đầu quá trình mã hóa ổ cứng của bạn.

Khi quá trình hoàn tất, ổ đĩa của bạn đã được mã hóa và bạn sẽ phải nhập mật khẩu mỗi lần khởi động máy tính.

Nếu bạn quyết định muốn loại bỏ mã hóa hệ thống trong tương lai, hãy khởi chạy giao diện VeraCrypt và nhấp vào **System > Permanently Decrypt System Partition/Drive.**

Trên đây là toàn bộ quy trình mã hóa ổ đĩa hệ thống Windows với VeraCrypt. Chúc các bạn thành công!