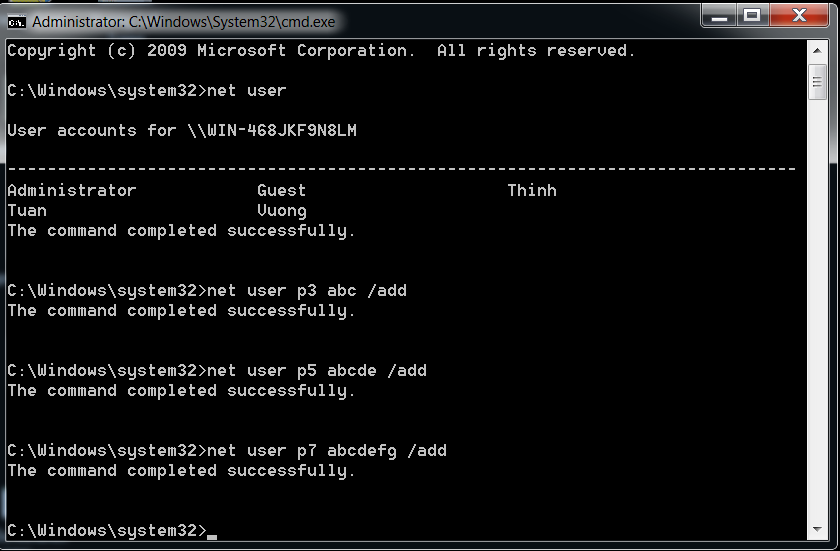
Lab-Project 12: Cracking Windows Passwords with Cain and Abel

Máy sử dụng: Windows 7

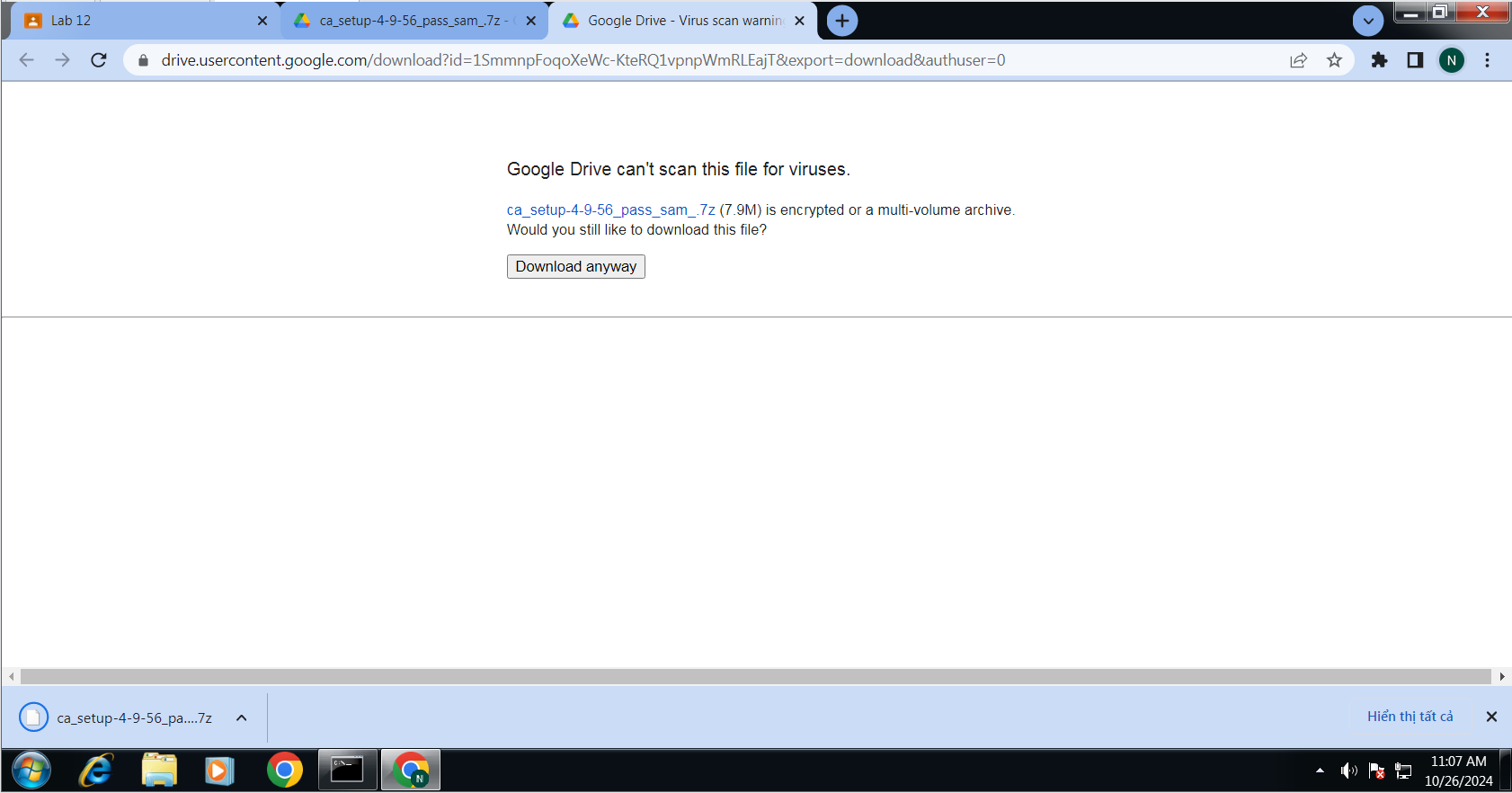
**Creating Passwords to Crack:**

* Sử dụng lệnh **net user** để tạo các user p3 (mk: abc); p5 (mk:abcde); p7 (mk:abcdefg)

****

**Downloading Cain & Abel:**

* Trên học liệu classroom; download file cài về

****

=> Cài đặt thành công

**Displaying the Password Hashes:**

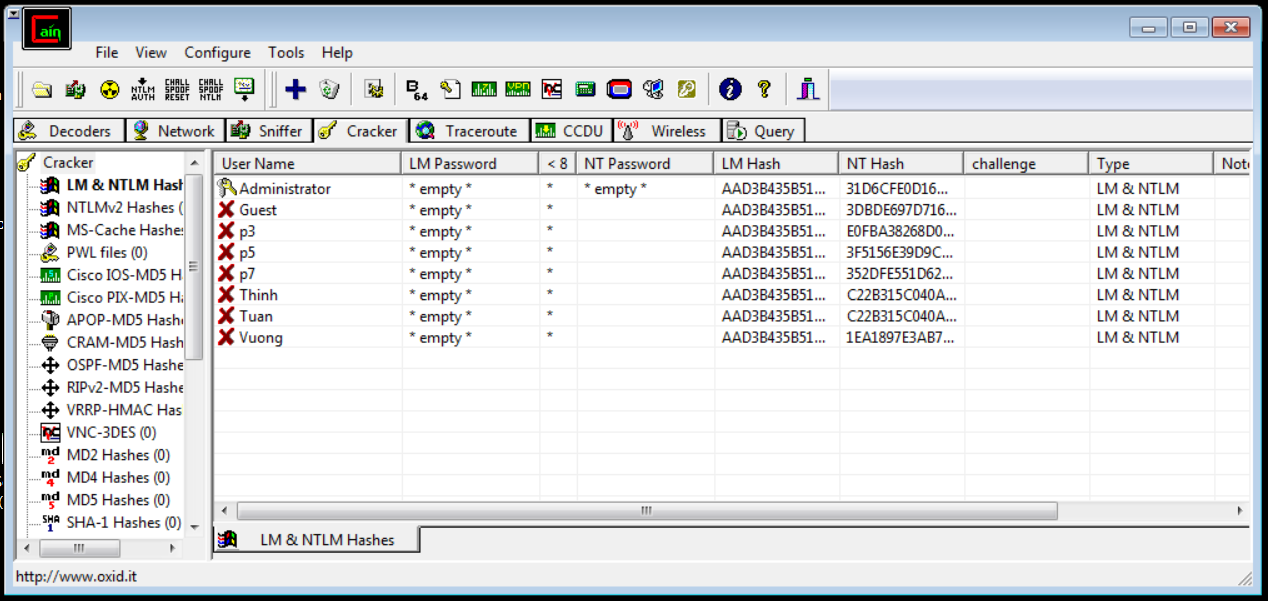
Nhấn **Start**, chọn **CAIN**.Cain trong kết quả tìm kiếm thì chuột phải và chọn **Run as Administrator** (Chạy với quyền Quản trị viên).

Nếu xuất hiện hộp thoại **User Account Control**, nhấn **Yes**.

Trong cửa sổ Cain, ở trên cùng, nhấp vào tab **Cracker**. Di chuyển chuột đến khu vực giữa bên phải, nơi có khung trắng trống với một lưới xám.

Nhấp chuột phải và chọn **Add to list** (Thêm vào danh sách). Trong hộp thoại **Add NT Hashes from**, nhấp Next.

Các giá trị hash của mật khẩu sẽ hiển thị như hình dưới đây. Các hash LM sẽ giống nhau nếu bạn đang sử dụng Windows Vista hoặc phiên bản mới hơn, nhưng NT hash chứa thông tin mật khẩu

****

**Cracking Passwords:**

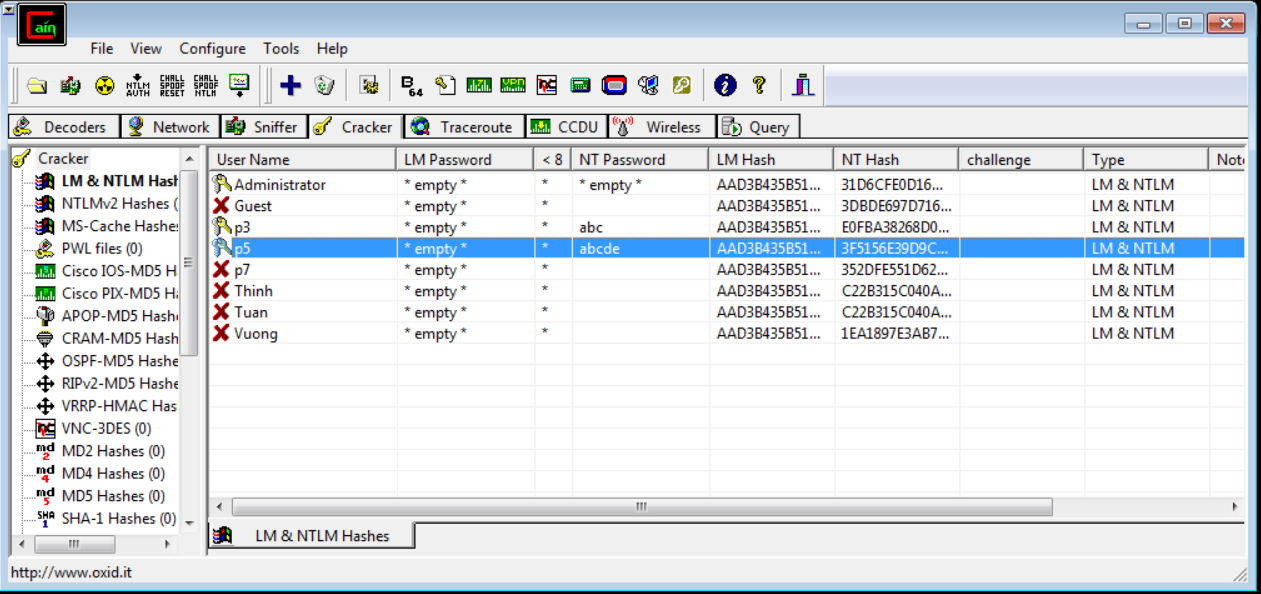
+ Trong khung bên phải, nhấp chuột phải vào **p3**, trỏ chuột đến **Brute-Force Attack** và chọn **NTLM Hashes**, như minh họa bên dưới trang này.

Lưu ý: chúng ta đang bẻ khóa các **NTLM hashes**, không phải các **LM hashes** cũ và yếu.

Các NTLM hashes khó bẻ khóa hơn nhiều, vì vậy phương pháp này chỉ hoạt động với các mật khẩu ngắn.

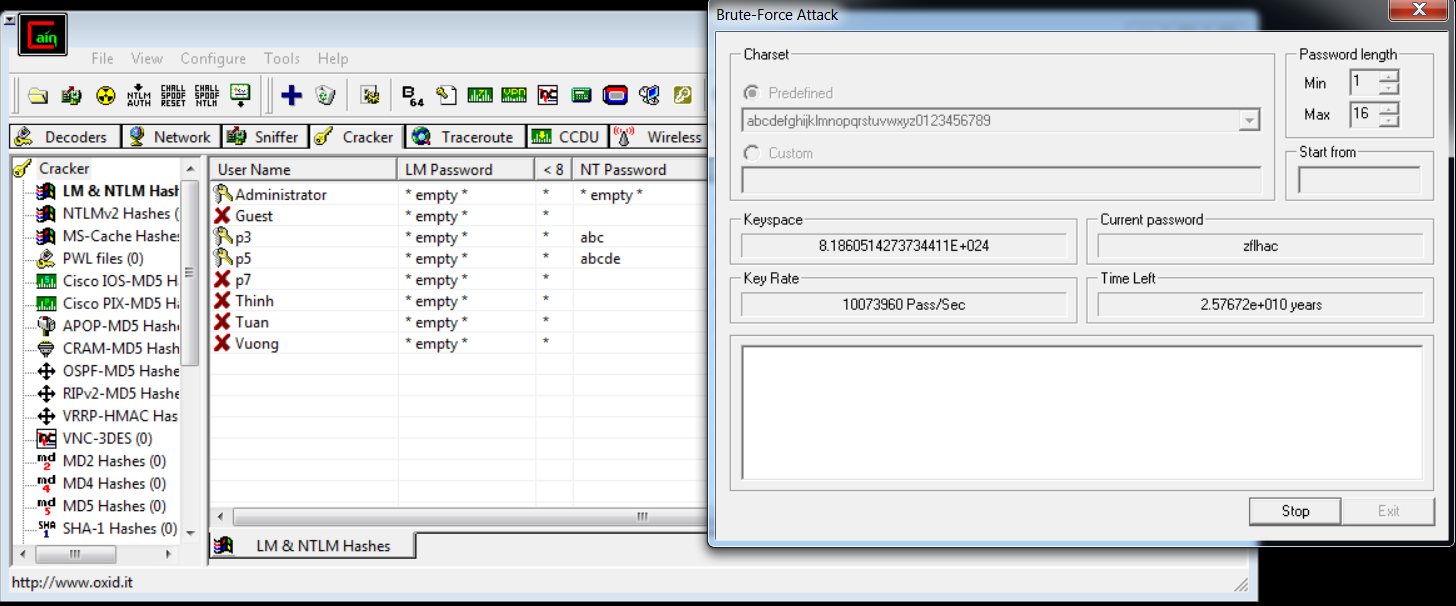
Trong hộp thoại **Brute-Force Attack**, nhấp vào nút **Start**. Chương trình sẽ tìm thấy mật khẩu ba ký tự ngay lập tức. Đóng hộp thoại **Brute-Force Attack**

+ Làm tương tự với p5

****

=> Kết quả của p3 và p5

+ Đến p7 cũng làm tương tự nhưng thời gian hiển thị mã hóa sẽ rất lâu

****