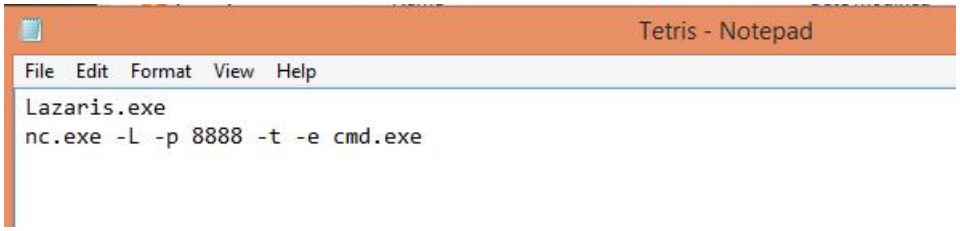
MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỤA
MAHP: CT222**02**

THỰC HÀNH - AN TOÀN HỆ THỐNG

Bài 04:

*** Remote Access Trojans (RATs):**



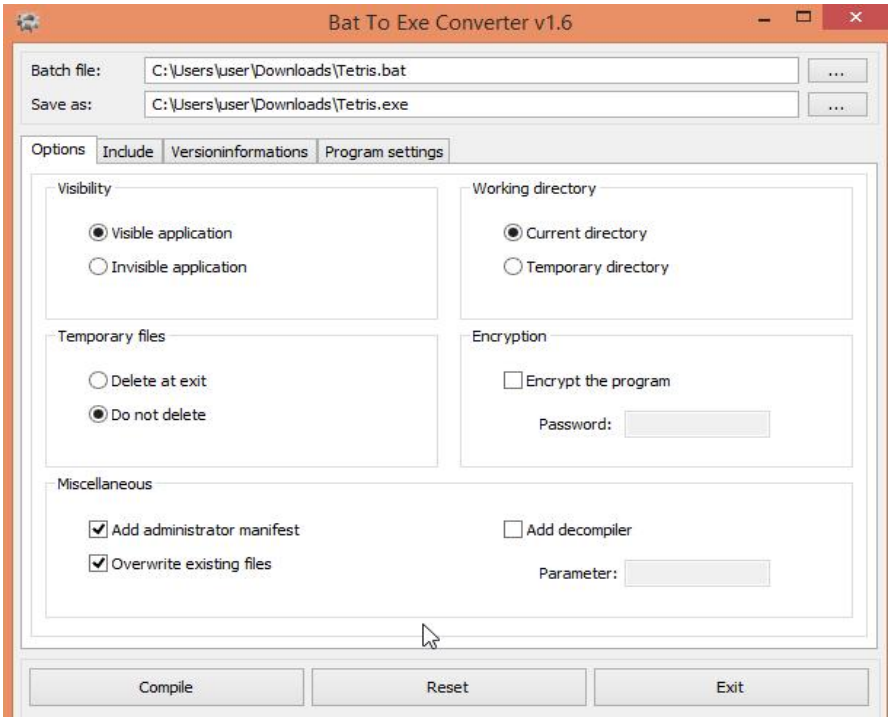
Hình 1: Nội dung kịch bản

- Bước 1: Đóng gói (Wrapper)

Chọn file Tetris.bat lưu thành Tetris.exe

+) Chọn các *Options*:

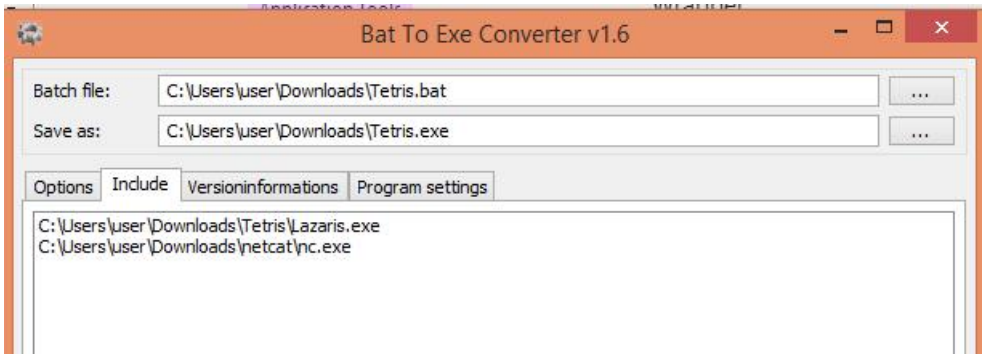
1) *Visble application*: Cho hiển thị ứng dụng (Nên sử dụng *Invisble application*);
2) *Current directory*: Chọn nơi lưu trữ gần nhất;
3) *Do not delete*: Không cho xóa dấu vết (Nên sử dụng *Delete at exit*);
4) *Add administrator manifest*: Sử dụng với quyền Quản trị;
5) *Overwrite existing files*: Cho phép ghi đè lên các file đã tồn tại.



Hình 2: Nội dung Options

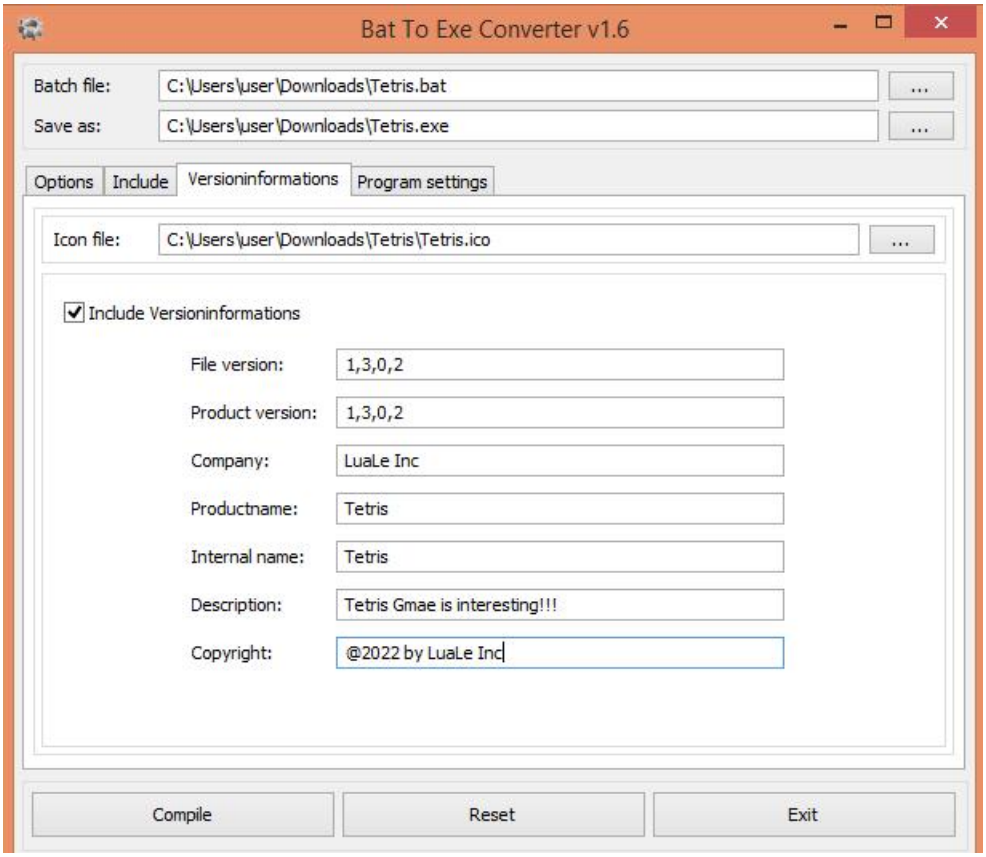
MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỤA
MAHP: CT222**02**

+) Đóng gói Tetris/Lazaris.exe và netcat/nc.exe:



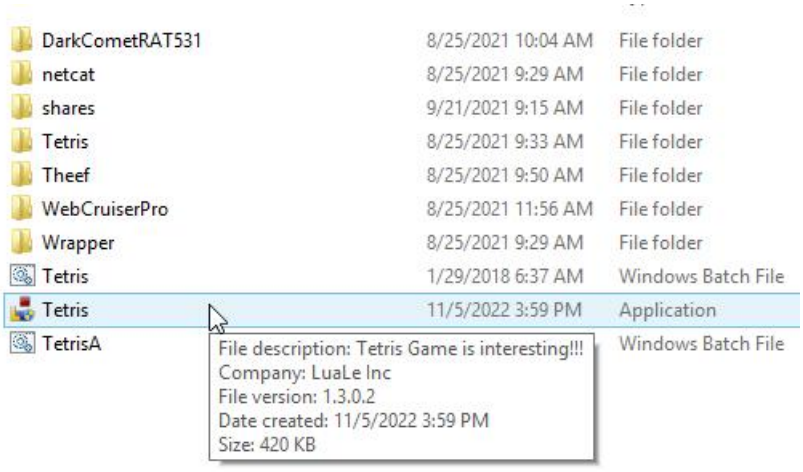
Hình 3: Nội dung Include

+) Tạo lớp ngụy trang cho ứng dụng:



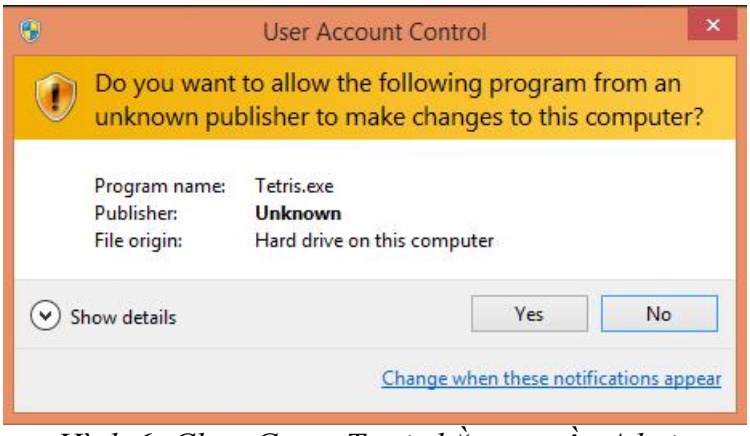
Hình 4: Nội dung Versioninformations

MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỤA
MAHP: CT222**02**

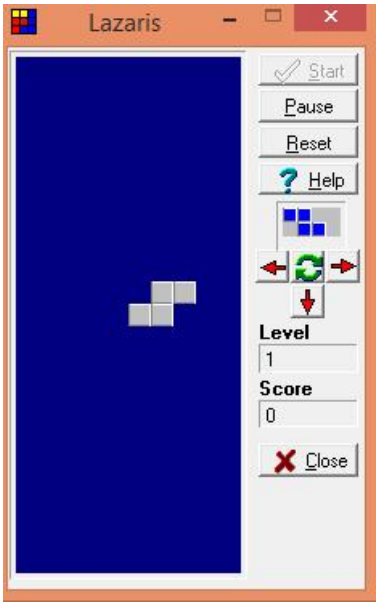


Hình 5: Tạo Game Tetris thành công

- Bước 2: Chạy ứng dụng

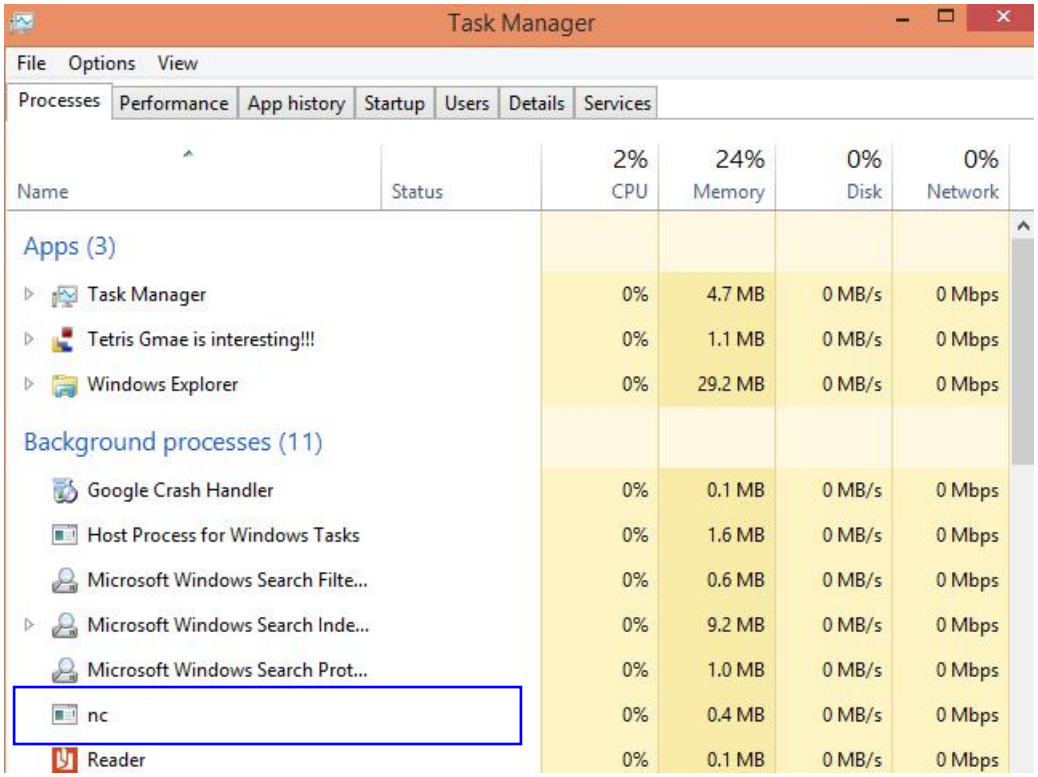


Hình 6: Chạy Game Tetris bằng quyền Admin

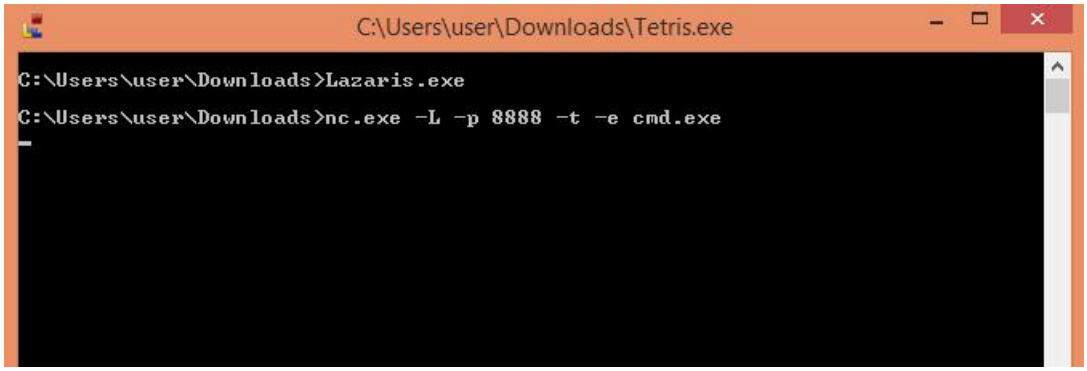


Hình 7: Chạy Game Tetris thành công

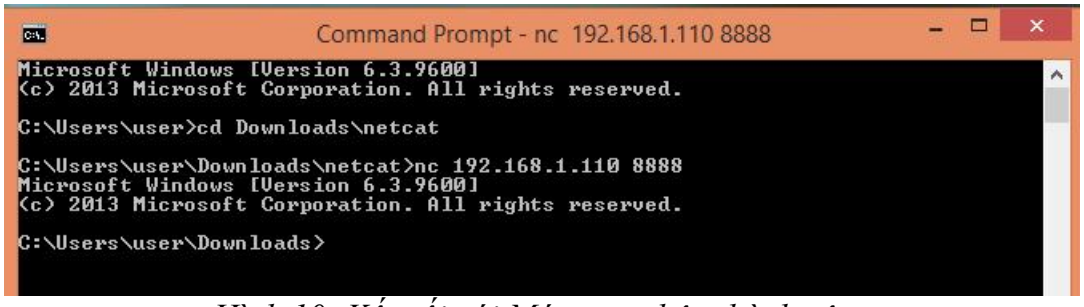
MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỤA
MAHP: CT222**02**



Hình 8: nc.exe chạy ngầm thành công



Hình 9: Tetris.exe chạy được nội dung kịch bản



Hình 10: Kết nối với Máy nạn nhân thành công

MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỤA
MAHP: CT222**02**

*** Trojan chuyên dụng (Theef):**

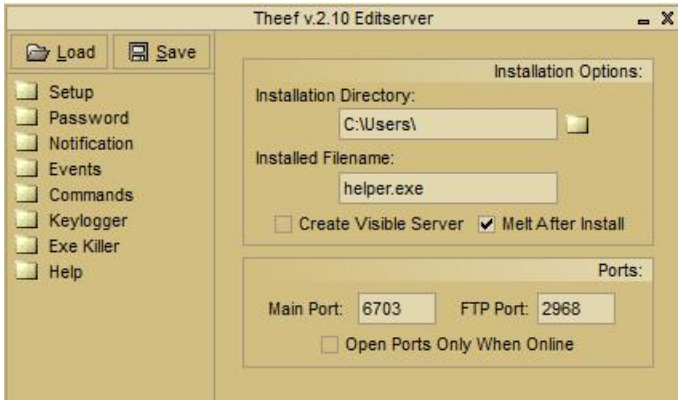
Hình 11: Nội dung kịch bản

- Bước 1: Bắt đầu Editserver

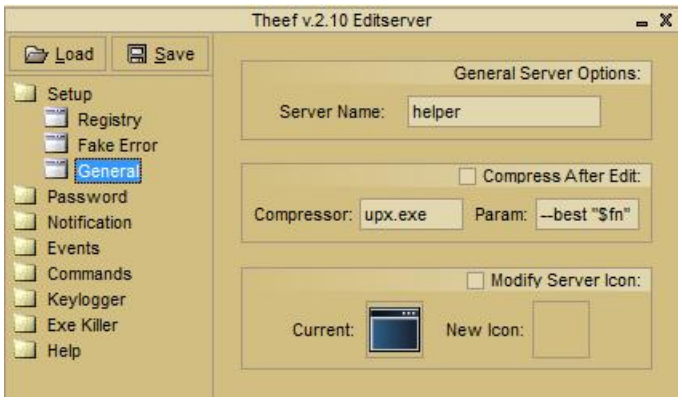
+) Nạp Server210;

1) Chọn nơi lưu trữ dễ dàng (máy nào cũng có);
2) Đặt tên cho file helper.exe;
3) Có cổng sau: 6703;
4) Cổng FTP: 2968 (ngẫu nhiên để đánh lừa);
5) Server Name: helper;

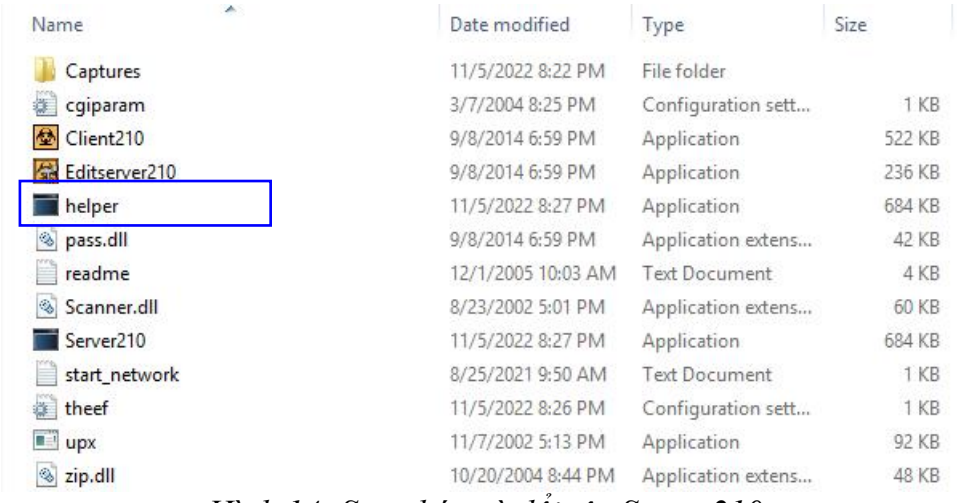
+) Save: Lưu chỉnh sửa



Hình 12: Nội dung chỉnh sửa

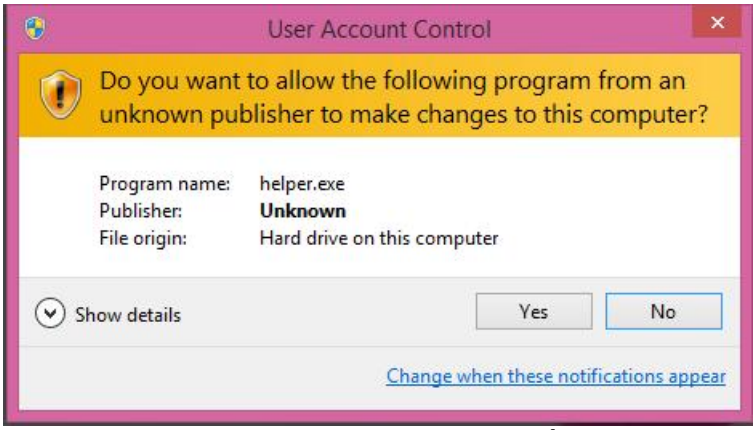


Hình 13: Nội dung chỉnh sửa

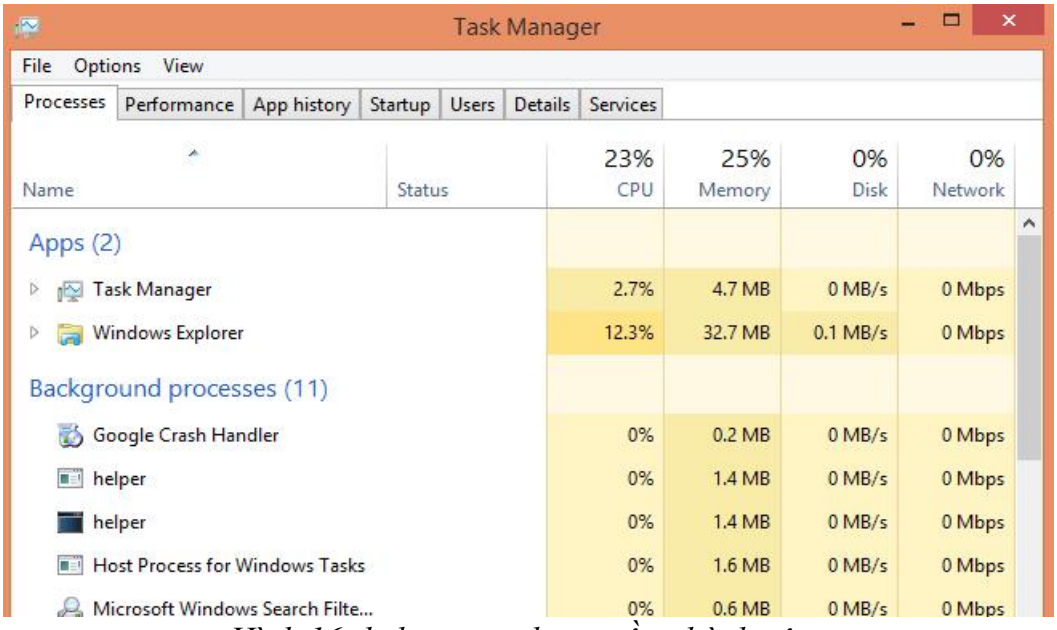


Hình 14: Sao chép và đổi tên Server210

- Bước 2: Chạy ứng dụng

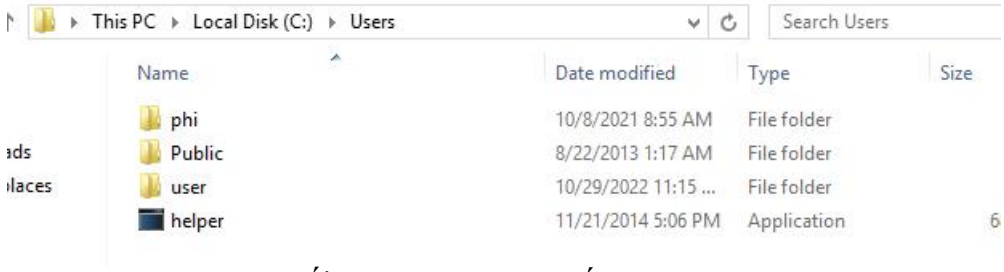


Hình 15: Chạy ứng dụng với quyền Admin



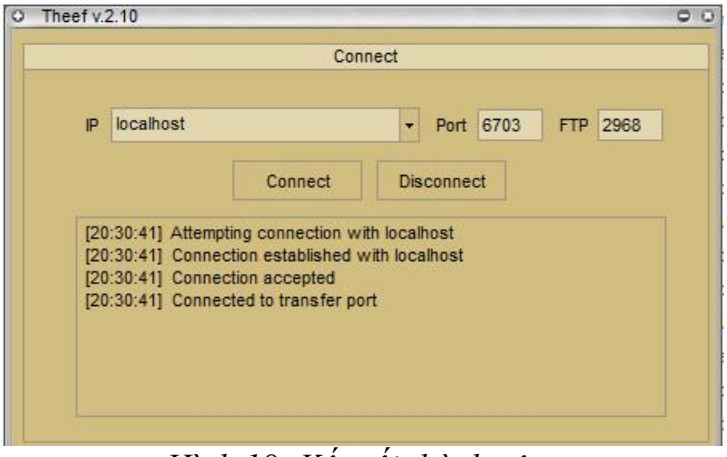
Hình 16: helper.exe chạy ngầm thành công

MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỤA
MAHP: CT222**02**

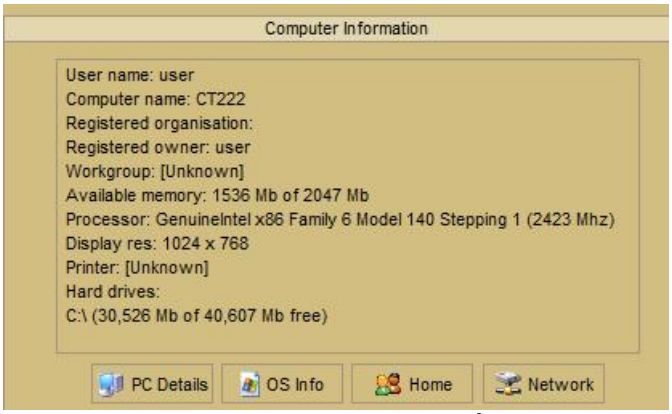


Hình 17: Ứng dụng helper xuất hiện trong Users

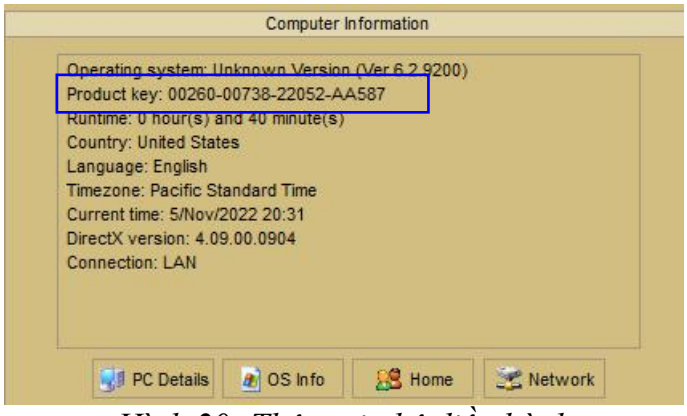
- Bước 3: Chạy Client210 để kết nối đến Máy nạn nhân để đọc dữ liệu, thông tin



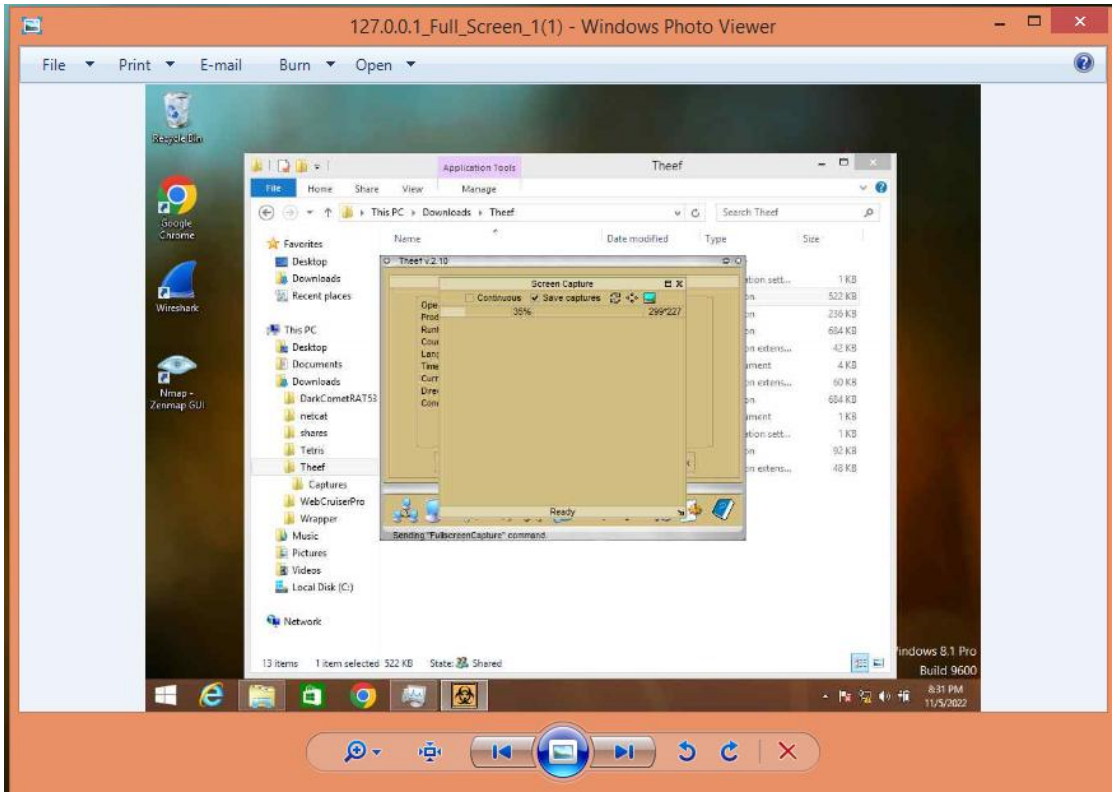
Hình 18: Kết nối thành công



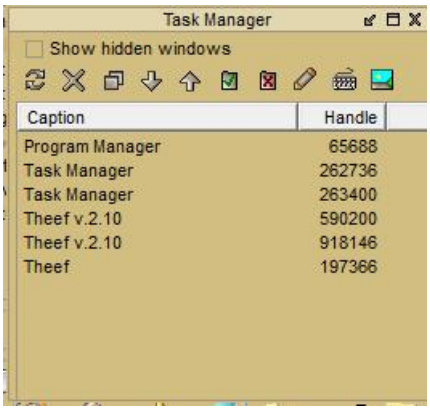
Hình 19: Thông tin chi tiết máy



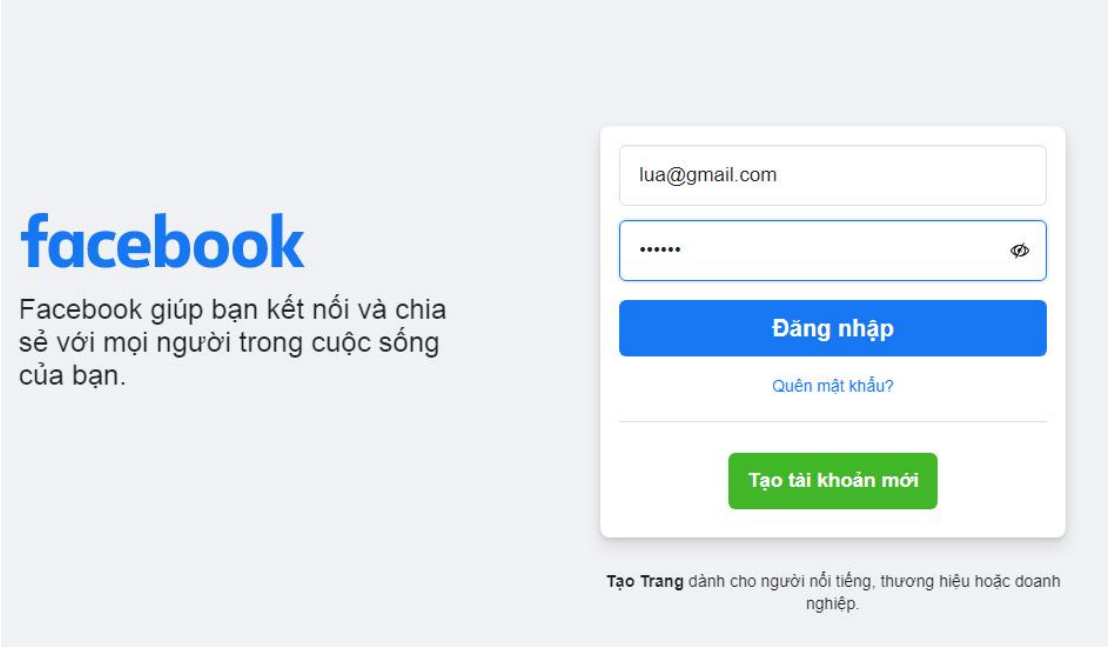
Hình 20: Thông tin hệ điều hành



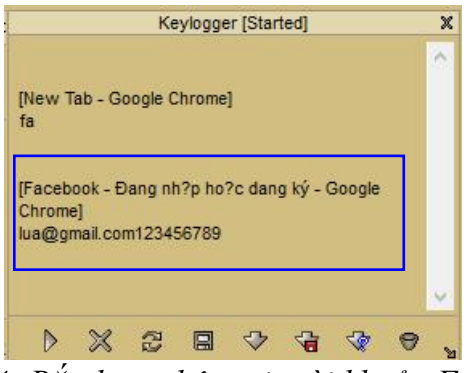
Hình 21: Capture màn hình



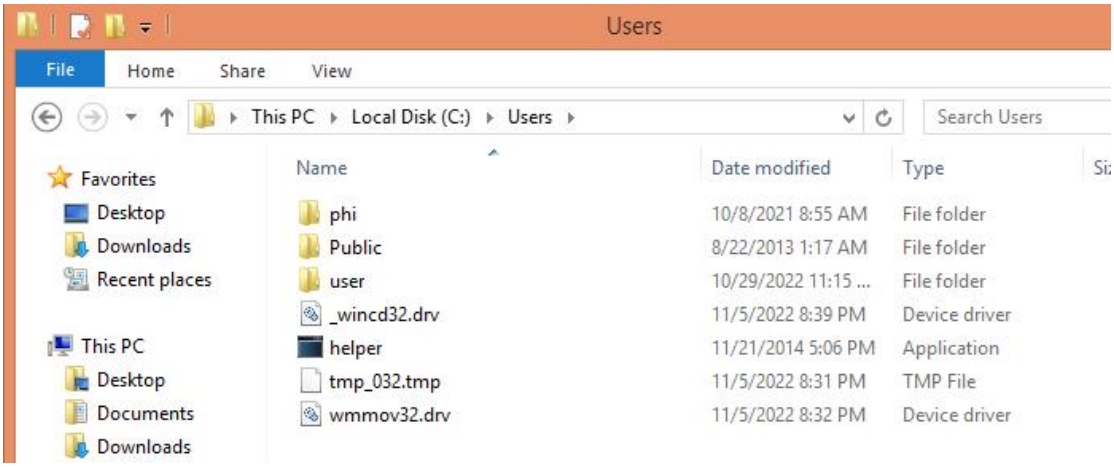
Hình 22: Xem các chương trình đnag chạy



Hình 23: Đăng nhập tài khoản Facebook



Hình 24: Bắt được thông tin tài khoản Facebook



Hình 25: Các file độc hại xuất hiện trong Users