HiddenTreasure:

Đây là file thực thi window 32 bit.



Pseudocode sau khi đã thực hiện chỉnh các hàm và kiểu dữ liệu:

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generatedGraphical user interface, text, application, Teams

Description automatically generated

Giải thích hoạt động:

Chương trình nhận vào thêm 2 tham số dòng lệnh:

arg[1] là đường dẫn file ảnh BMP (tại dòng 68 có check 2 byte đầu của file có phải là “BM”).

arg[2] là chuỗi bất kì. Chuỗi bất kì này sẽ được giấu ở trong file ảnh bmp.

Flag đã được giấu trong file ảnh inside-the-mind-of-a-hacker-memory.bmp sử dụng chương trình này. Cần phải tìm hiểu hoạt động của chương trình để xem cách giấu, từ đó lấy được flag từ file ảnh ra.

Flow chương trình có thể được chia làm hai phần chính:

Phần 1: cấp phát 1 vùng nhớ có độ lớn gấp 8 lần độ lớn của arg[2] (theo byte). Mỗi byte của vùng nhớ này sẽ có dạng 0000 000X, trong đó X là 1 bit của arg[2], lần lượt theo thứ tự tới hết. (1 byte có 8 bit nên cần 1 vùng nhớ gấp 8 lần arg[2]).

Phần 2:

Chương trình thực hiện tìm địa chỉ của Pixel array của file bmp.

Pixel array được cấu tạo theo dạng bảng có hàng và cột. Độ dài của hàng và cột được cung cấp trong phần bmp header. (Chương trình cũng đã trích xuất những thông số này, tạm gọi là W và H). Mỗi phần tử của bảng đại diện cho 1 điểm ảnh, độ dài 3 byte, mỗi byte đại diện cho 1 màu R, G, B.

Chương trình thực hiện giấu data vào file ảnh như sau:Chọn hàng 0, 3, 6, .... Với mỗi pixel của dòng đó, ghi đè 1 byte của buffer ở bước 1 (thực ra chính là giấu 1 bit của arg[2]) vào byte đầu tiên của pixel. (Nếu hết hàng 0 mà chưa hết nội dung cần giấu thì tiếp tục ở hàng số 3, tuy nhiên nội dung của flag là ngắn so với số pixel của 1 hàng nên ta không quan tâm lắm), cứ tiếp tục như vậy cho tới khi hết arg[2].

Thực hiện đọc file theo đúng thứ tự này ở file ảnh đã được cung cấp sẽ được flag:

flag{dont\_forget\_the\_treasure}

