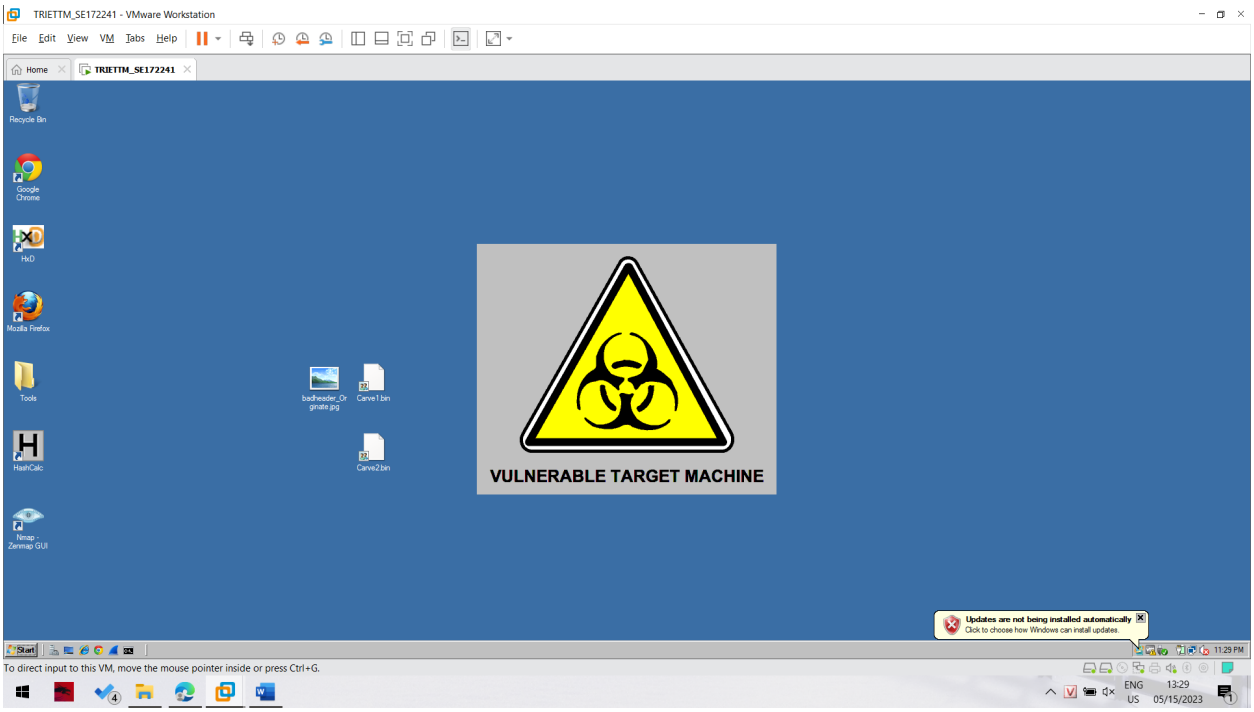
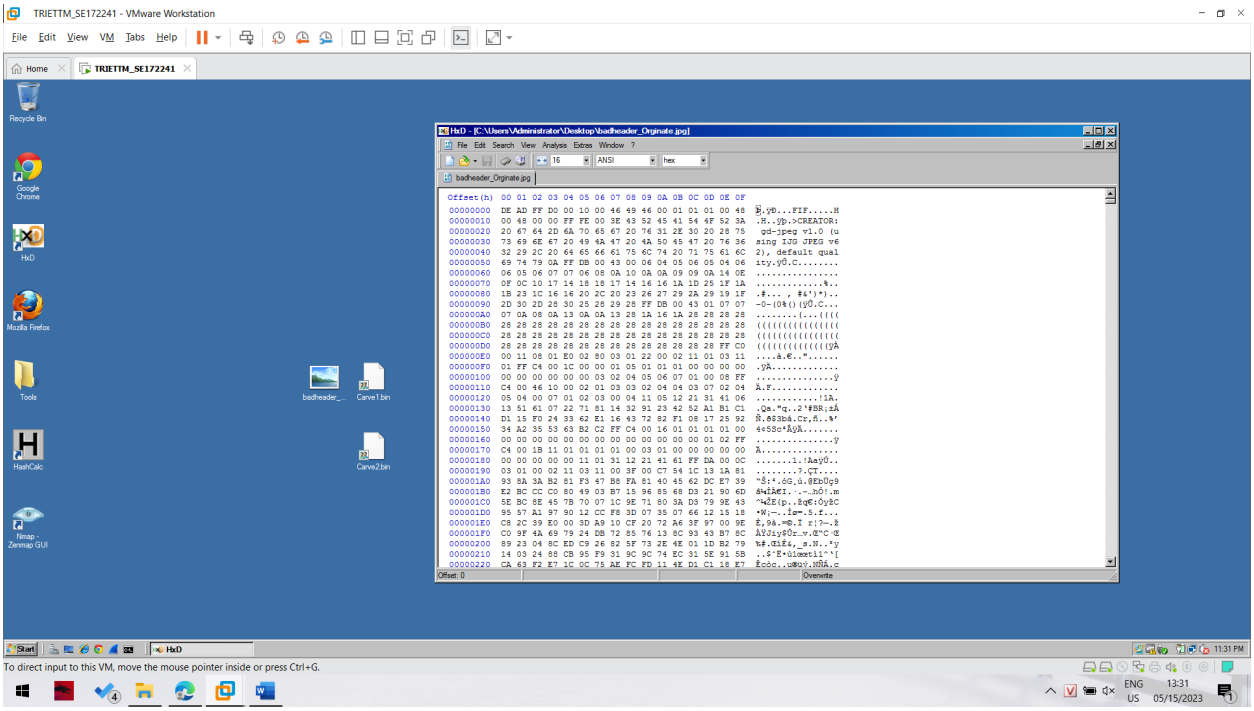
Lab 1

Ở bài lab này chúng ta sẽ tiền hành khôi phục ba tấm hình bằng công cụ HxD. Thông qua việc khôi phục header cảu chúng, ta có thể xem được ba tấm ảnh ban đầu.



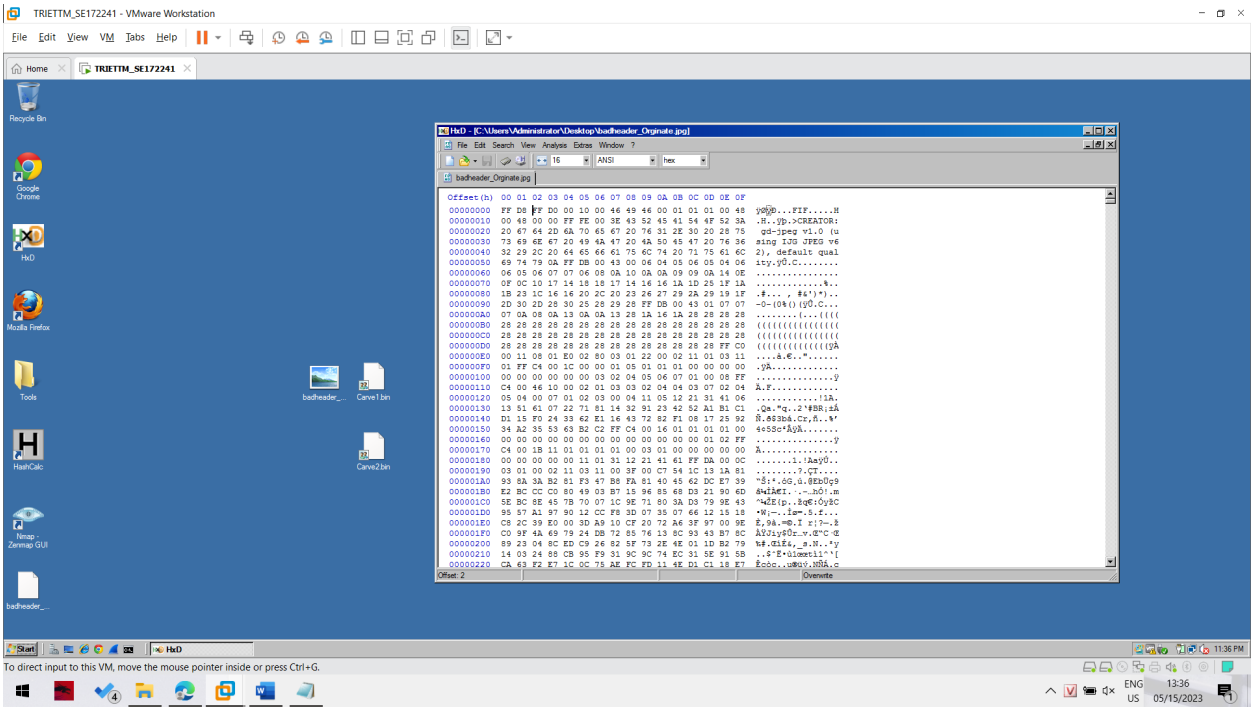
Ba tấm ảnh lần lượt là badheader.jpg, Carve1.bin, Carve2.bin.

Đầu tiên ta sẽ tiến hành khôi phục tấm ảnh badheader.jpg

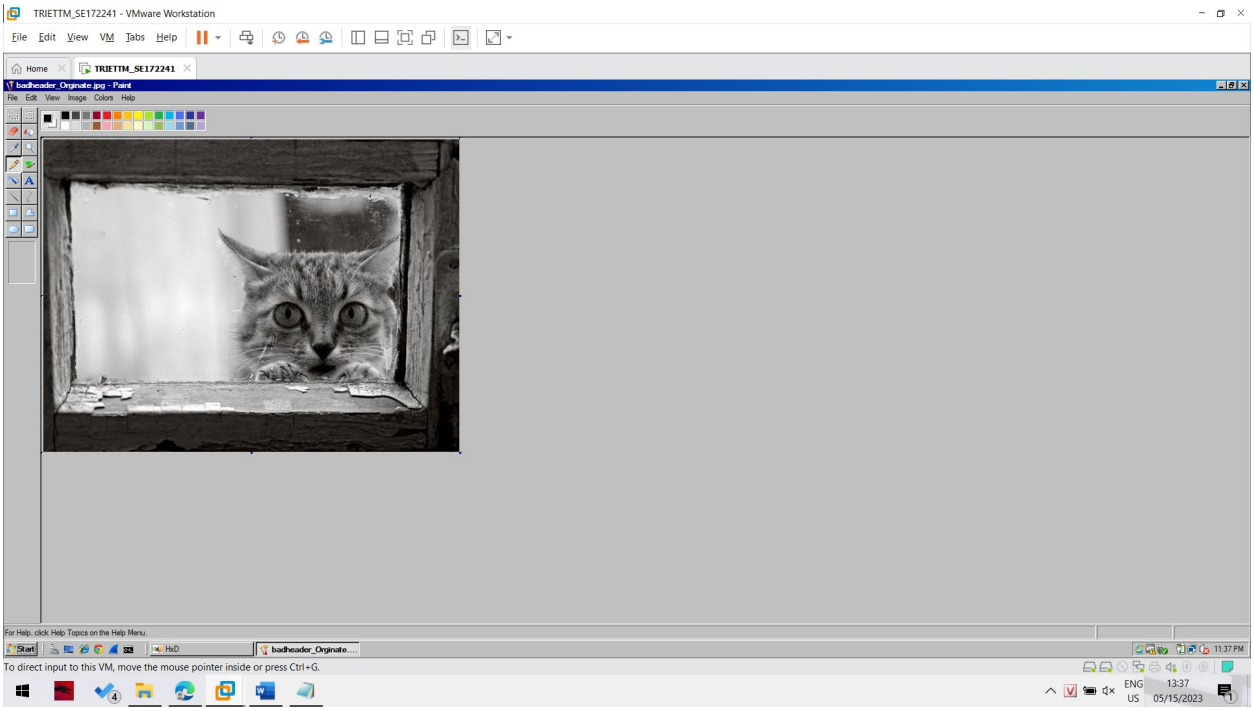


Nhận thấy tấm ảnh này có đuổi extension là jpg, nên ta tiến hành google một chút tìm được magic number của loại file này là FF D8 FF.

Nhìn màn hình hex của HxD, ta thấy header này đã bị chỉnh sửa, và cũng chính vì magic number bị sai nên ta không mở hình này lên xem được. Ta tiến hành sửa header này thành magic number đã tìm được.

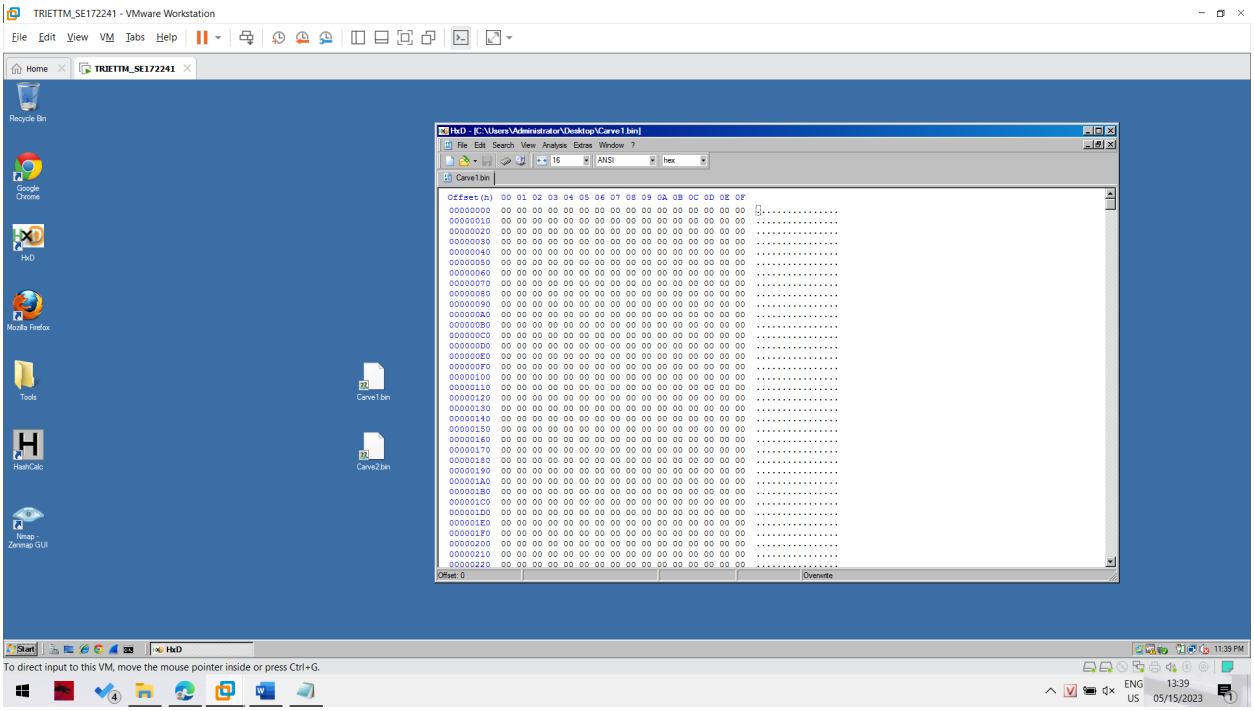


Sau khi sửa và save lại HxD tự tạo ra một file bak là file backup cũ đoạn hex ban đầu. Nhưng ta không cần quan tâm tới nó giờ thì mở tấm ảnh lên coi đã xem được chưa nào.



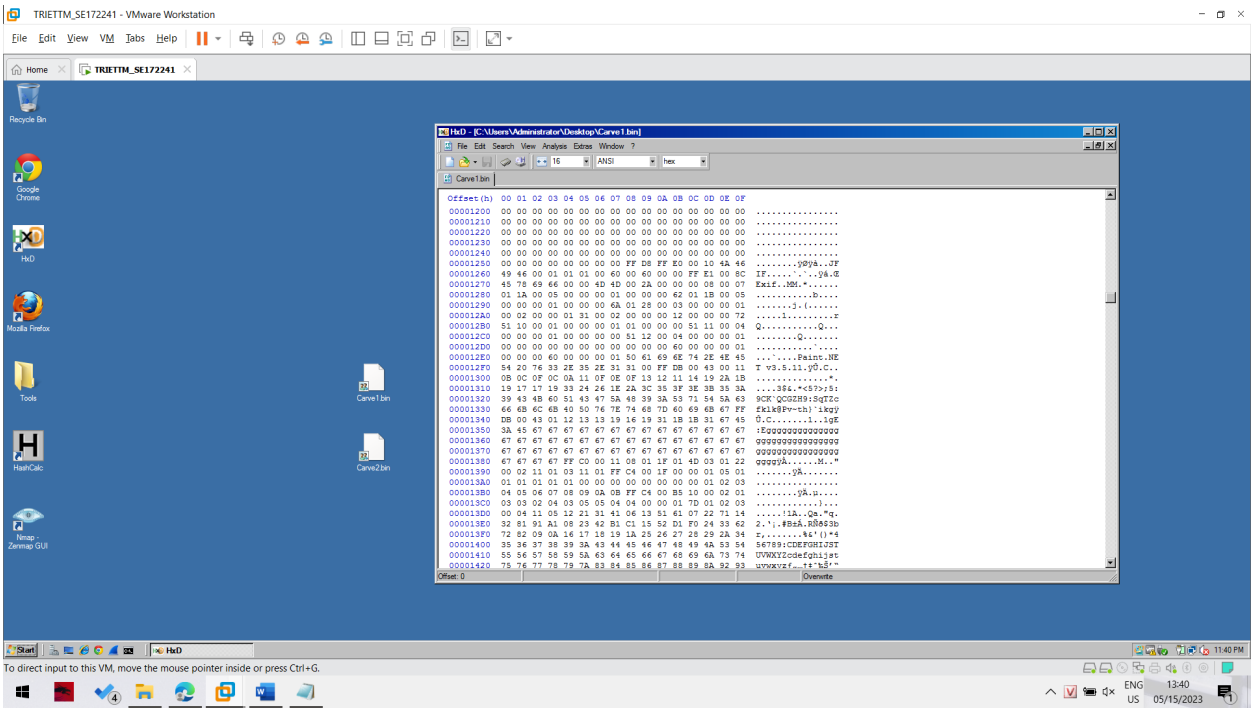
Tuyệt vời, vậy là ta đã khôi phục thành công tấm hình đầu tiên.

Tiếp theo là tấm ảnh Carve1.bin, ta tiến hành load nó vào HxD.

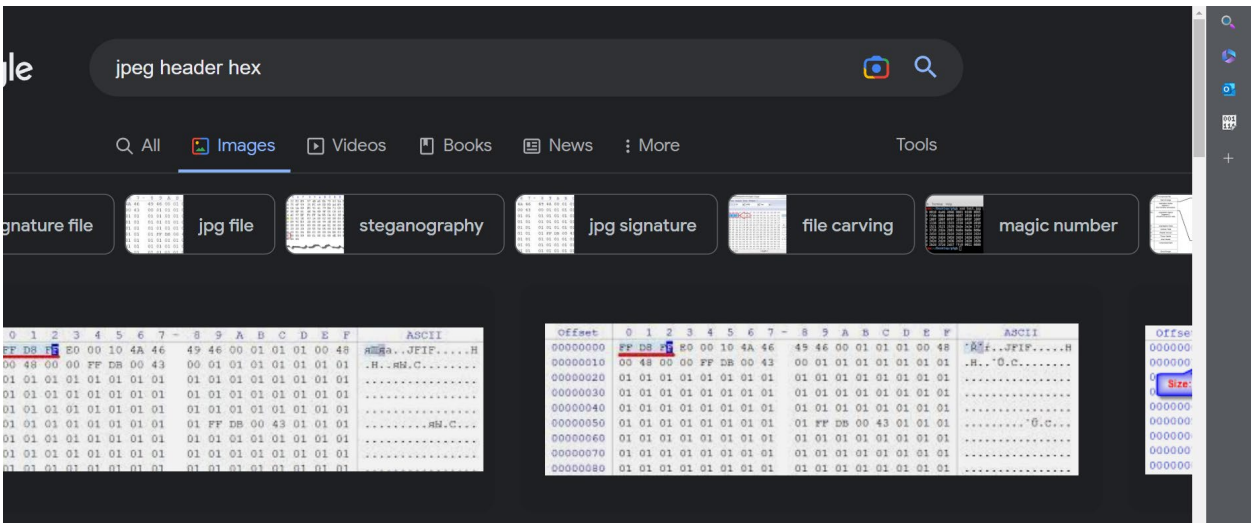


Lần này đề bài không cho ta biết trước đuổi file là gì mà chỉ để là .bin. Mặt khác màn hình hex của HxD thì toàn là số 0.

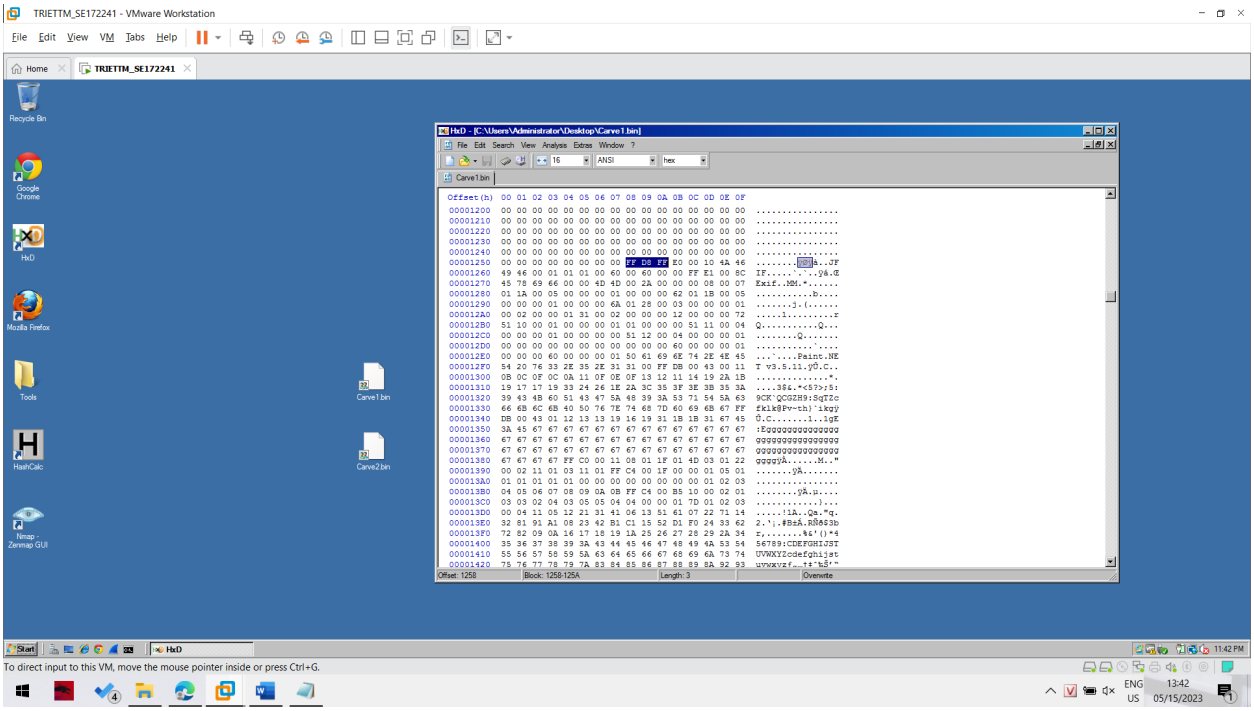
Ta tiến hành lướt qua đoạn hex này một chút.



Đến đoạn này là bắt đầu xuất hiện một số byte trên màn hình. Ta thấy có một số chữ khả nghi ở đây là JFIF. Đem google ta biết được thông tin như sau

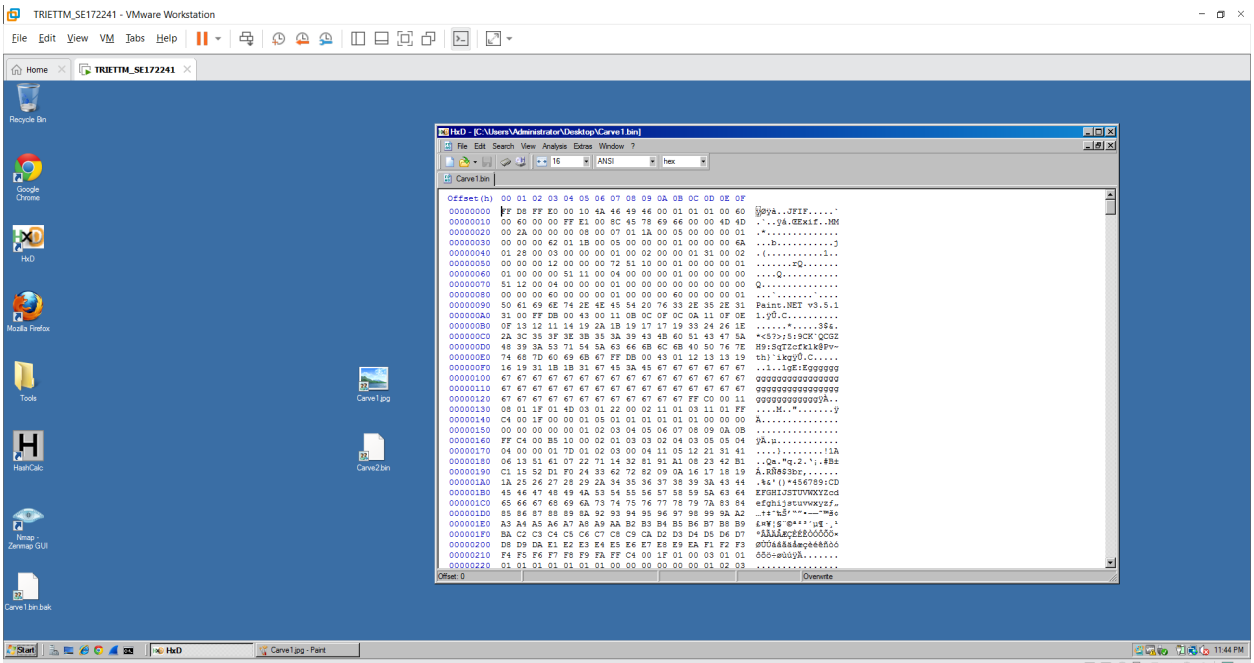


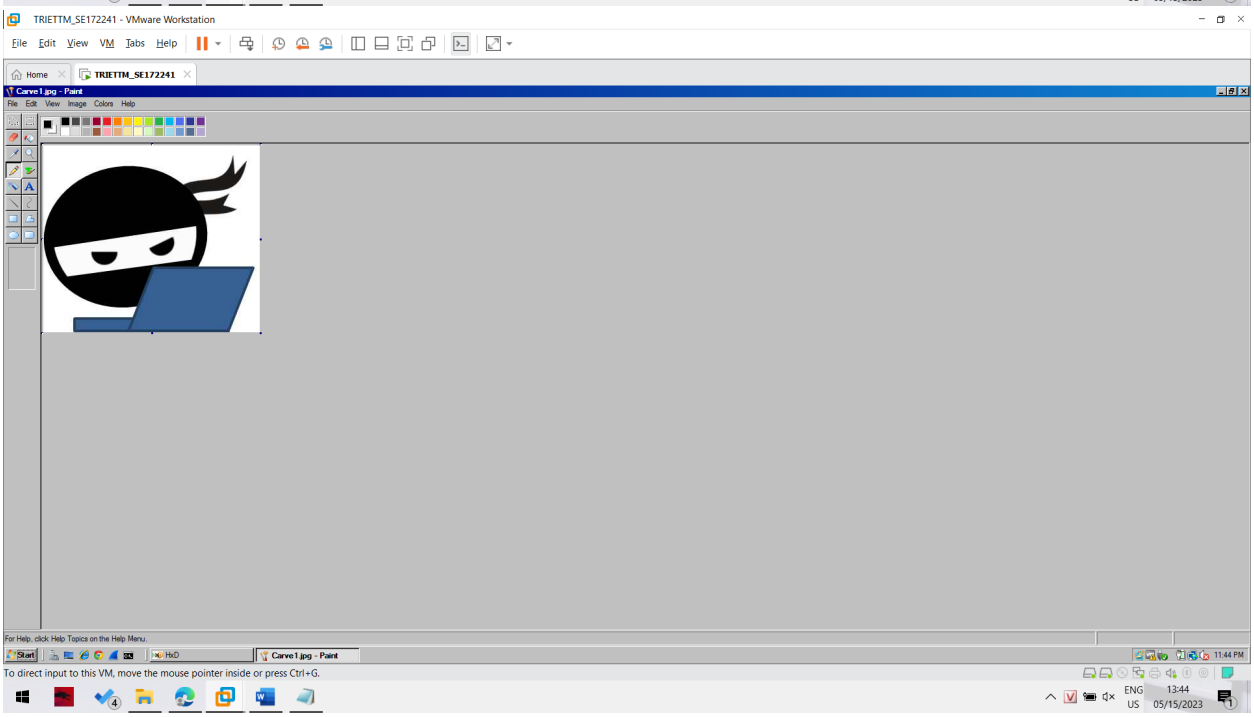
Ta thấy JFIF này là một phần của header file ảnh jpg. Vậy này chính là file ảnh jpg rồi. Nếu để ý kỹ màn hình hex, magic number của file jpg cũng ở ngay đây luôn.



OK vậy có nghĩa là đống byte 0 phía trên là vô nghĩa nên ta sẽ tiến hành xóa bỏ nó đi.

Save lại rồi đổi đuổi file từ bin thành jpg, mở file lên ta nhận được tấm hình đã được khôi phục.

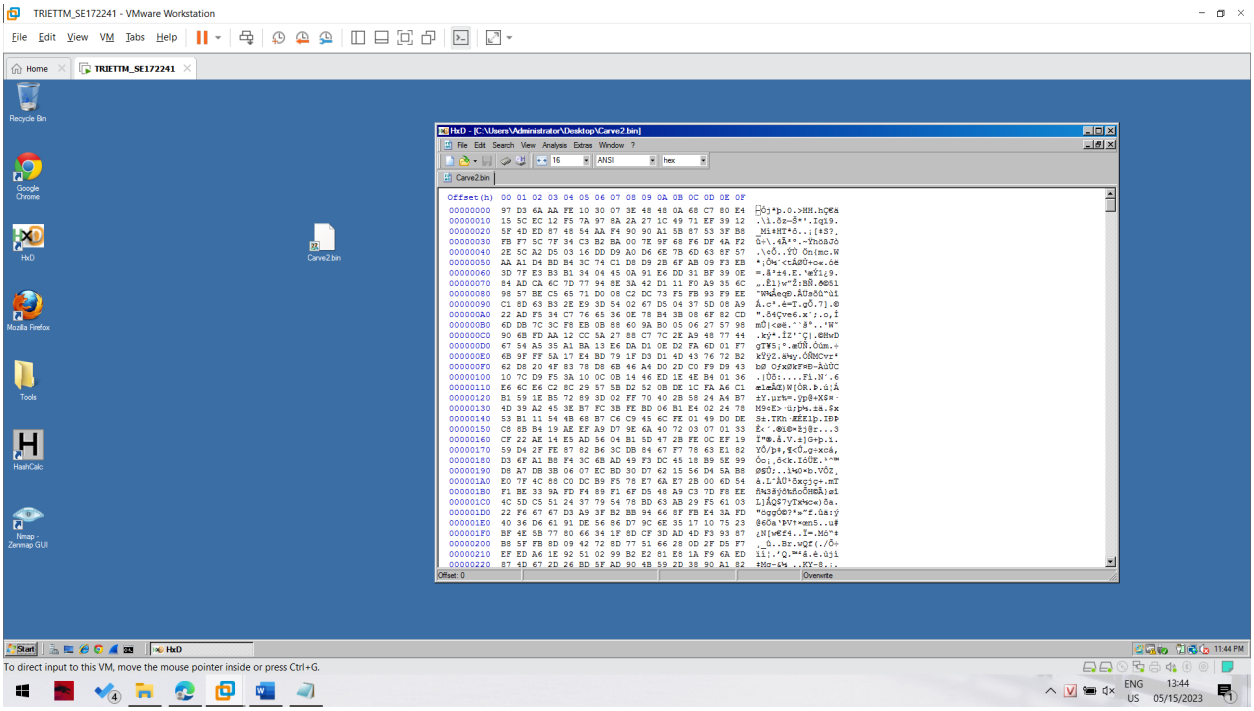




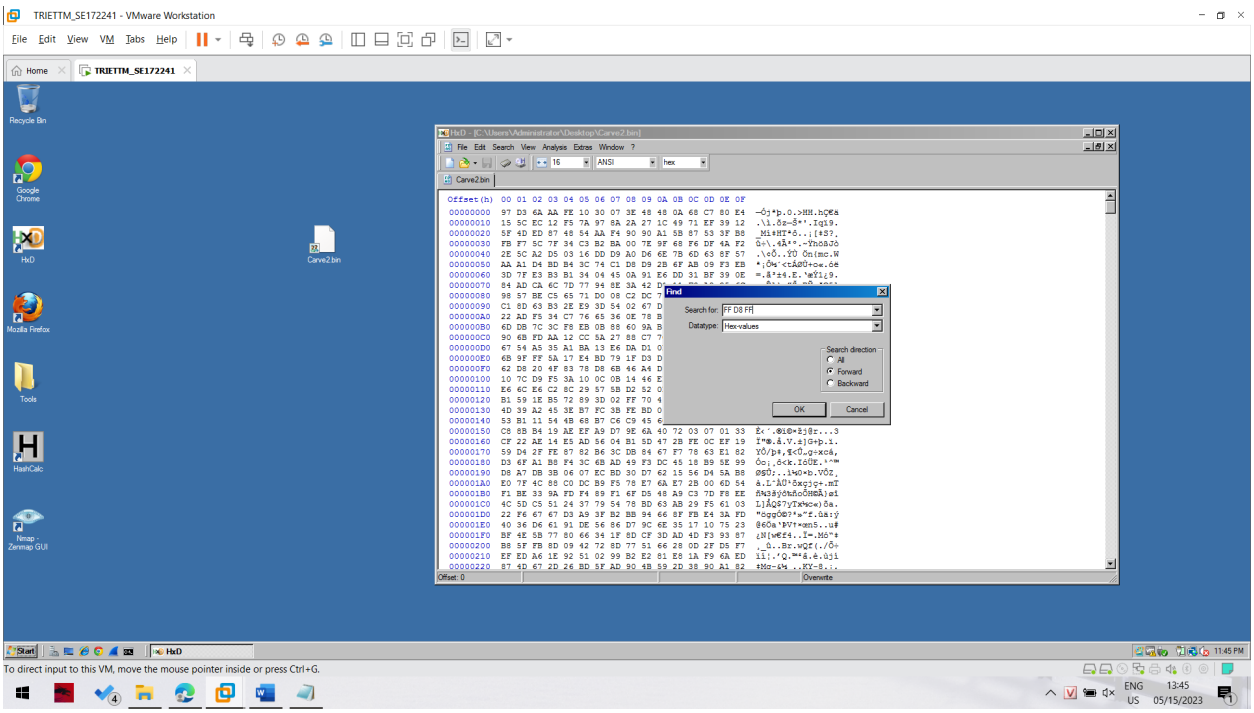
Ngon, vậy là ta đã khôi phục thành công tấm hình thứu hai rồi.

Tiếp đến tấm hình cuối cùng.

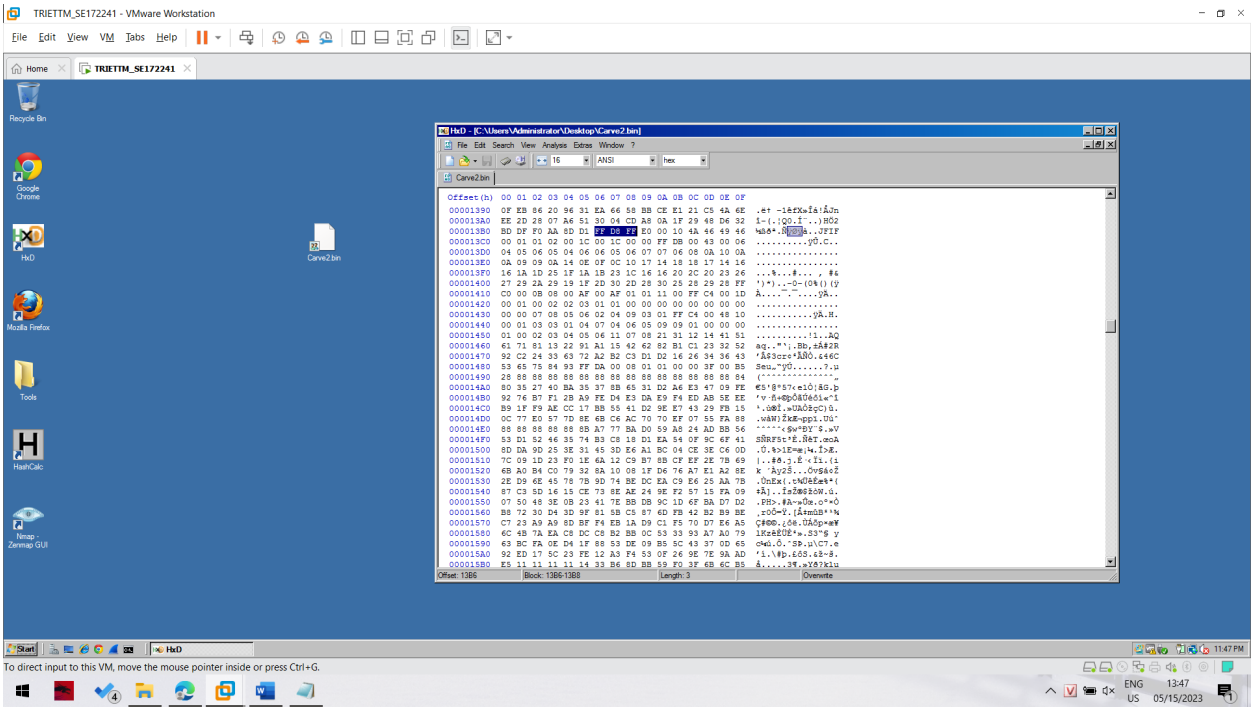
Load tấm Carve2.bin là HxD ta thấy một đống byte



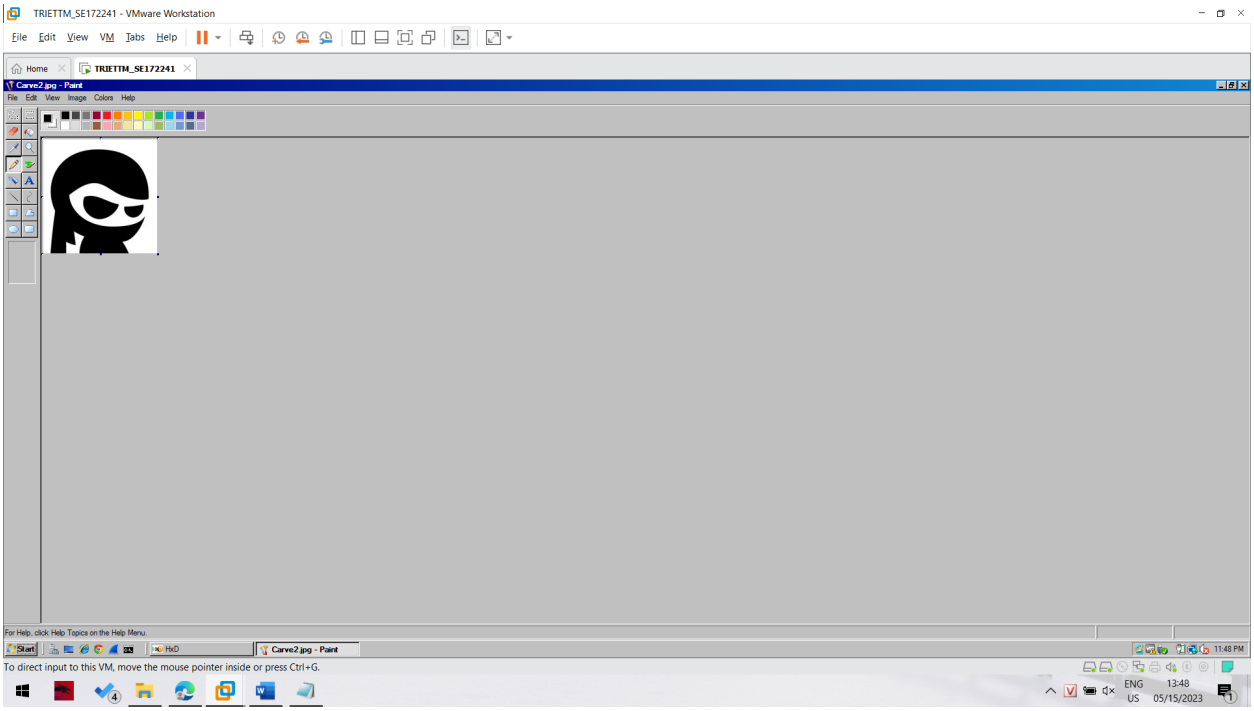
Đến đây ta sẽ sử dụng chức năng của công cụ HxD này là search để tìm kiếm coi có header jpg có ở đây không.



Chọn như trên màn hình rồi search



Ta tìm được một header jpg, vậy là này vẫn là ảnh jpg. Ta làm y như tấm trước xóa đống byte vô nghĩa ở phía trên đi.



Cuối cùng ta khôi phục được tấm ảnh thứ 3.