**Catrupted Revenge Challenge Write-up by RandomTeuz**

1. **Giới thiệu**

Catrupted Revenge là challenge có độ khó Easy, nằm trong mảng Forensics (điều tra số), yêu cầu ta tìm Flag từ một tệp tin có tên cat.png

Icon

Description automatically generated

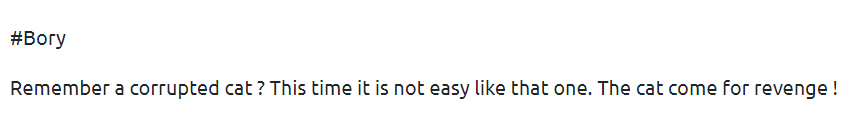
1. **Phân tích**

* PNG là định dạng phổ biến dùng cho các file hình ảnh
* Ngay từ thumnail của file ta đã không thấy được hình ảnh thu nhỏ nào và khi mở file lên kiểm tra cũng nhận được lỗi hệ thống không hỗ trợ định dạng file này.

Graphical user interface, text

Description automatically generated

* File thì không mở được, vậy phải nhờ tới đề bài rồi



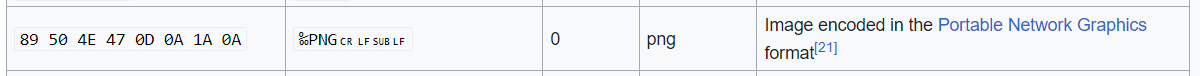
* Theo đề bài giải thích thì dường như file đã bị hỏng ở đâu đó
* Với hướng tiếp cận của một newbie cả ở việc chơi CTF lẫn mảng Forensics thì lựa chọn lúc này của mình là nhờ ông chú Google hỗ trợ.
* Và đây là trang hỗ trợ mình tìm được (<https://trailofbits.github.io/ctf/forensics/>). Trong đó phân đoạn quan trọng nhất đập vào mắt mình là:

### “File format identification (and "magic bytes")

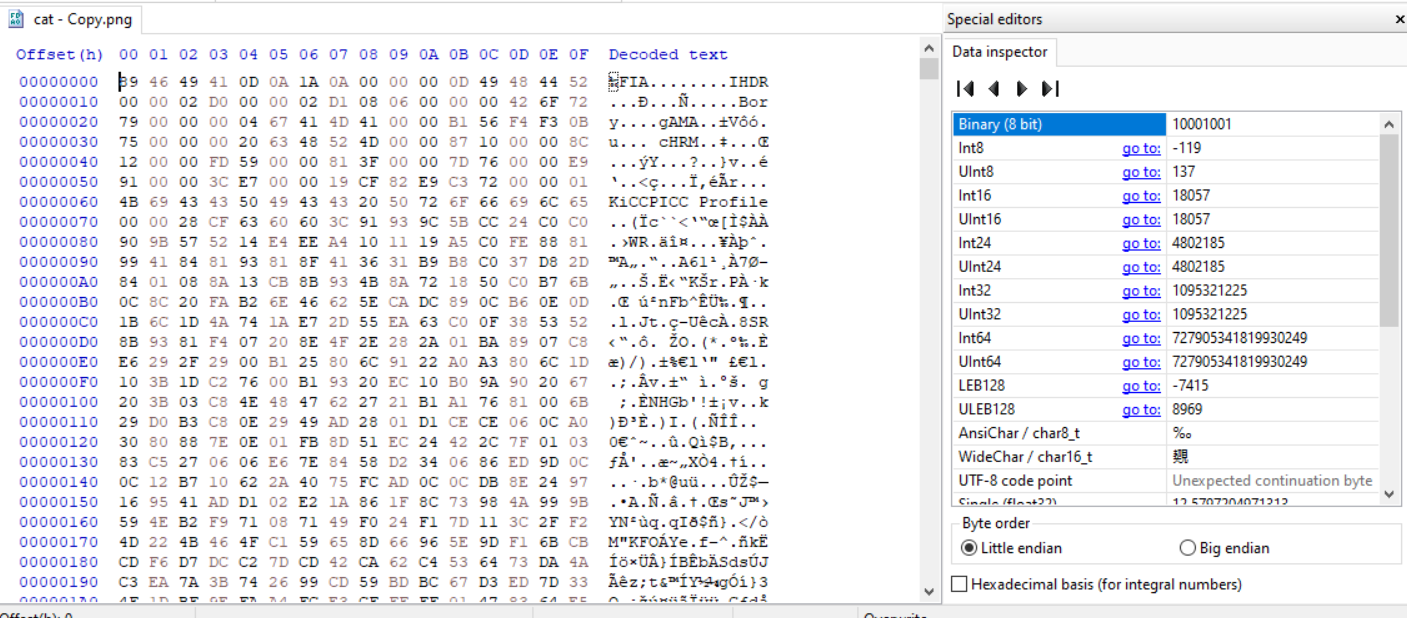
Almost every forensics challenge will involve a file, usually without any context that would give you a guess as to what the file is. Filetypes, as a concept for users, have historically been indicated either with filetype extensions (e.g., readme.md for MarkDown), MIME types (as on the web, with Content-Type headers), or with metadata stored in the filesystem (as with the mdls command in MacOS). In a CTF, part of the game is to identify the file ourselves, using a heuristic approach.

The traditional heuristic for identifying filetypes on UNIX is libmagic, which is a library for identifying so-called "magic numbers" or "magic bytes," the unique identifying marker bytes in filetype headers. The libmagic libary is the basis for the file command.”

* Đoạn này đề cập tới khái niệm magic number là một file header đặc trưng xác định định dạng file. Vậy tiếp tục sử dụng “magic number” làm từ khóa để tìm kiếm và mình tìm được (<https://en.wikipedia.org/wiki/List_of_file_signatures>)
* Task file là Cat.png vậy nên ta note lại Magic Number của file PNG



* Đường link bên trên cho ta một danh sách các magic number tương ứng với từng loại file. Định dạng của magic number có vẻ là số Thập lục phân (HEX). Do đó hướng đi tiếp theo là thử mở file dưới dạng thập lục phân.
* HxD Hex Editor là một chương trình được phát triển bởi Mael Horz. Như một trình soạn thảo hex, nó có thể truy cập và các tập tin thay đổi hex, mà có nghĩa là nó có thể được sử dụng cho các nhiệm vụ như thẩm định hồ sơ, kiểm tra hồ sơ, kiểm tra đĩa và sửa chữa, kiểm tra log file.
* Sử dụng HxD để mở Task File



* Ta để ý thấy dãy 8 chữ số HEX đầu tiên của file, khi so sánh với Magic number của file PNG, thì chỉ có 5 số là đúng

Task File: Decoded text:

Text

Description automatically generated A picture containing box and whisker chart

Description automatically generated

PNG Magic Number:



* Do đó ta sửa lại 3 số đã bị thay đổi

Text

Description automatically generated with low confidence

* Và Decoded text cũng thay đổi, có vẻ file đã được khôi phục về đúng định dạng PNG?

A picture containing icon

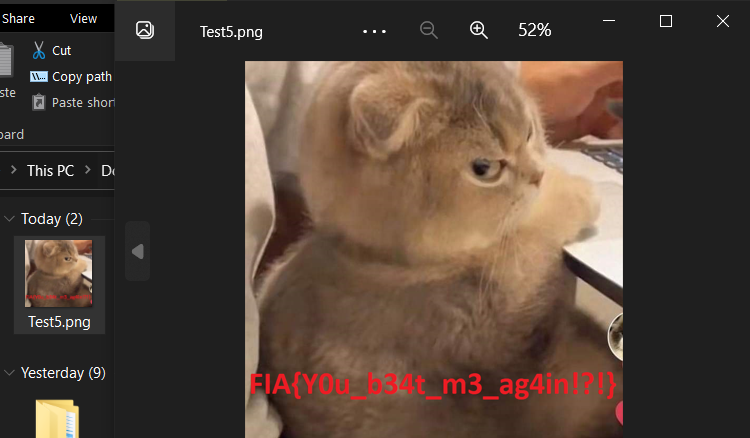
Description automatically generated

* Lúc này ta tiến hành lưu file sau khi khôi phục với lựa chọn Save As -> Tên tùy thích

A picture containing text

Description automatically generated

* Task File sau khi được khôi phục sẽ cho chúng ta biết Flag



Flag: FIA{Y0u\_b34t\_m3\_ag4in!?!}

1. **Kết**

KIỂM TRA MAGIC NUMBER CỦA FILE ĐI!!