Forensics cũng là một dạng mà mình practice khá nhiều, chắc nhiều hơn cả mảng web vì vậy sau khi thất bại ở chall web thì mình quay xe sang forensics ngay lập tức. Tiếc là ở mảng này mình lại mất quá nhiều thời gian vào các câu lý thuyết ☹

1. Hello Shark

A screenshot of a computer

Description automatically generated

Là một trong nhưng câu lý thuyết mình giải được, thì ở đây với kiến thức mình biết thì file pcap chính là viết tắt của từ Paket Capture Data vậy nên flag của bài này chính là : EHC{packetcapturedata}

1. Oh! Shark is cute!

A screenshot of a computer error

Description automatically generated

Đây là một câu lý thuyết rất cơ bản và đáp án chính là wireshark. Vì vậy đáp án của flag này chính là : EHC{wireshark}

1. Comment more command

A screenshot of a computer

Description automatically generated

Sau khi tải file swan.png và mở ra thì có hình chú thiên nga ở bên dưới

A screenshot of a screenshot of two swans

Description automatically generated

Không có gì đặc biệt ở bức ảnh này cả vậy nên mình sẽ sử dụng HXD để xem bên trong có gì

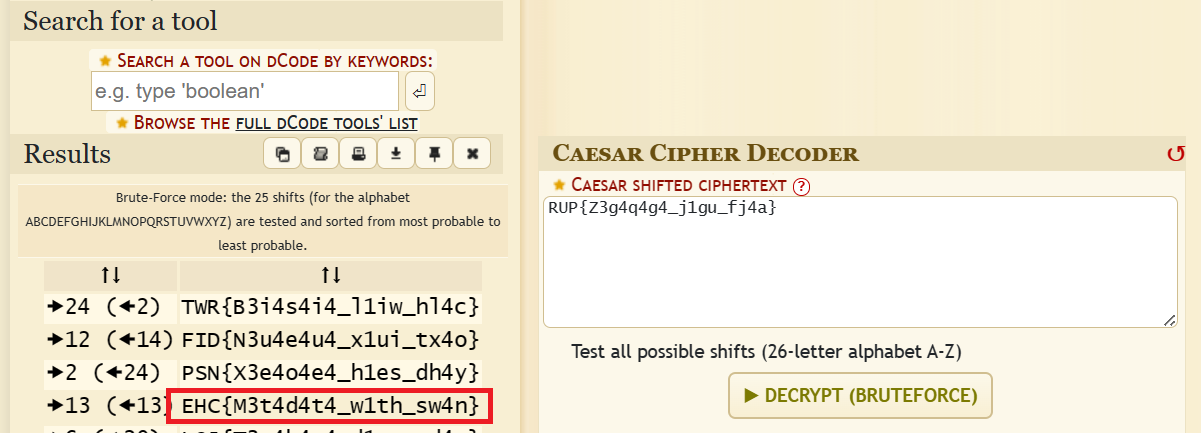
A screenshot of a computer

Description automatically generated

Có vẻ như Header đúng signature của file png rồi. Ở End Chunk cũng không có xáo trộn hay thêm bớt gì cho nên mình sẽ chuyển qua vmware và sử dụng exiftool để kiểm tra metadata của nó xem có gì bất thường không



Và mình đã tìm thấy flag ở phần artist nhưng flag đang bị encrypt và mình đoán đây là dạng cipher encryption. Vậy nên mình đã copy encrypted flag và mang lên cipher decoder online để decrypt và cho ra kết quả chính là flag mà mình cần tìm



Flag : EHC{M3t4d4t4\_w1th\_sw4n}

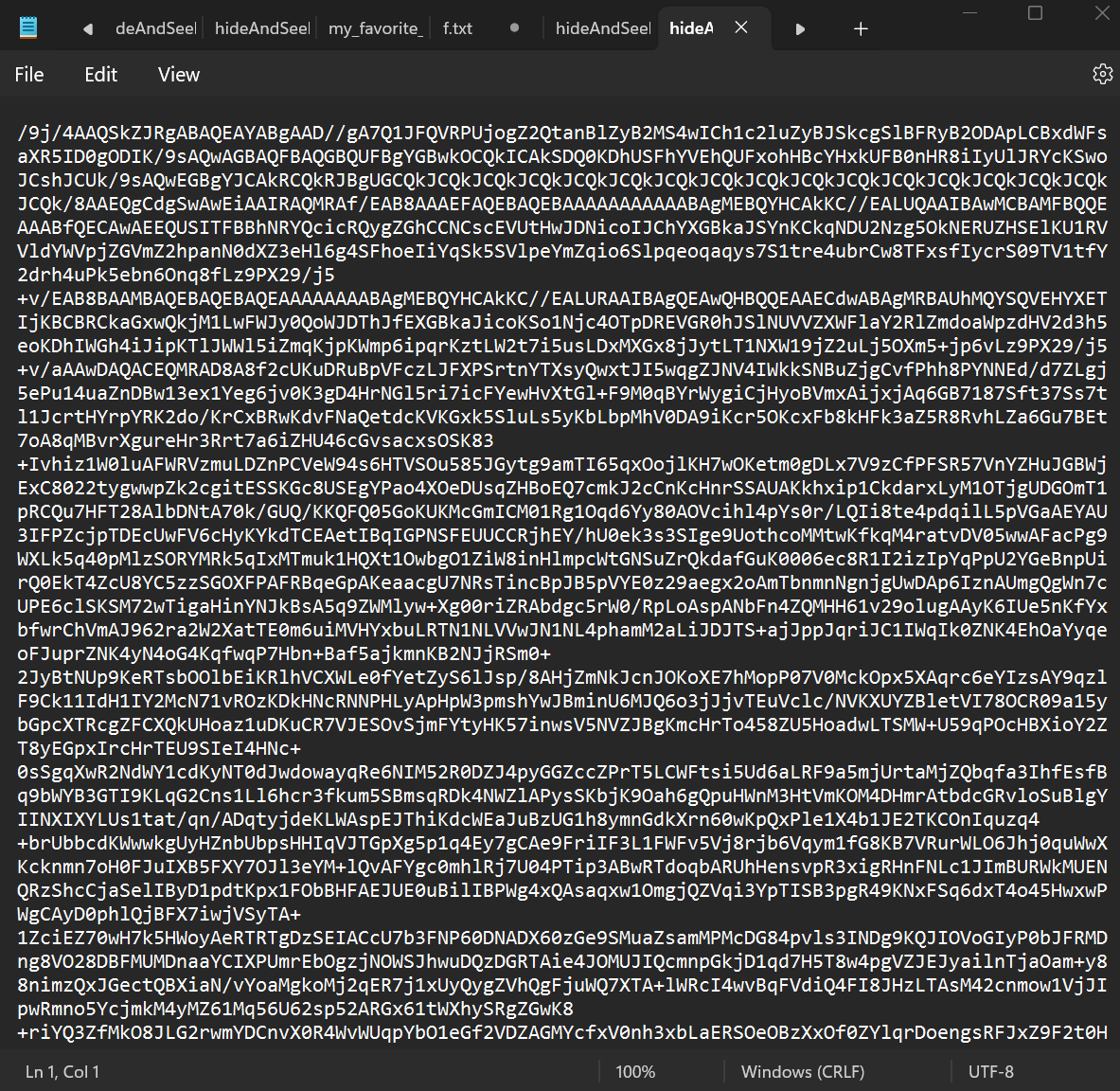
1. Cat&tulip. Hide&seek

A screenshot of a computer

Description automatically generated

Rất đang tiếc là chall này mình đã làm gần ra rồi nhưng do không để ý đề bài yêu cầu nên mình đã không nộp được flag ☹

Sau khi tải file hideAndSeek.txt về mình mở nó để xem và cho ra một đoạn text khá dài



Nhìn sơ qua thì có vẻ nó đang được mã hóa ở một dạng nào đó. Nhìn có vẻ rất giống base64 và theo kinh nghiệm của mình khi giải forensics thì đối với những bài có những đoạn text dài như này thì cứ copy paste lên các trang analyze ciphertext để xem chính xác nó ở dạng mã hóa nào.

A screenshot of a computer

Description automatically generated

Kết quả đúng như mong đợi nó đã analyze và xác định đoạn text này được mã hóa bằng base64

Copy text và decode bằng base64 thì mình đã có một đoạn text như sau :

A screenshot of a computer

Description automatically generated

Nhìn header thì đúng chính xác là file JPG rồi giờ mình sẽ lưu đoạn text decode này về và chuyển extension sang đuôi .jpg để xem nó là gì

A screenshot of a computer

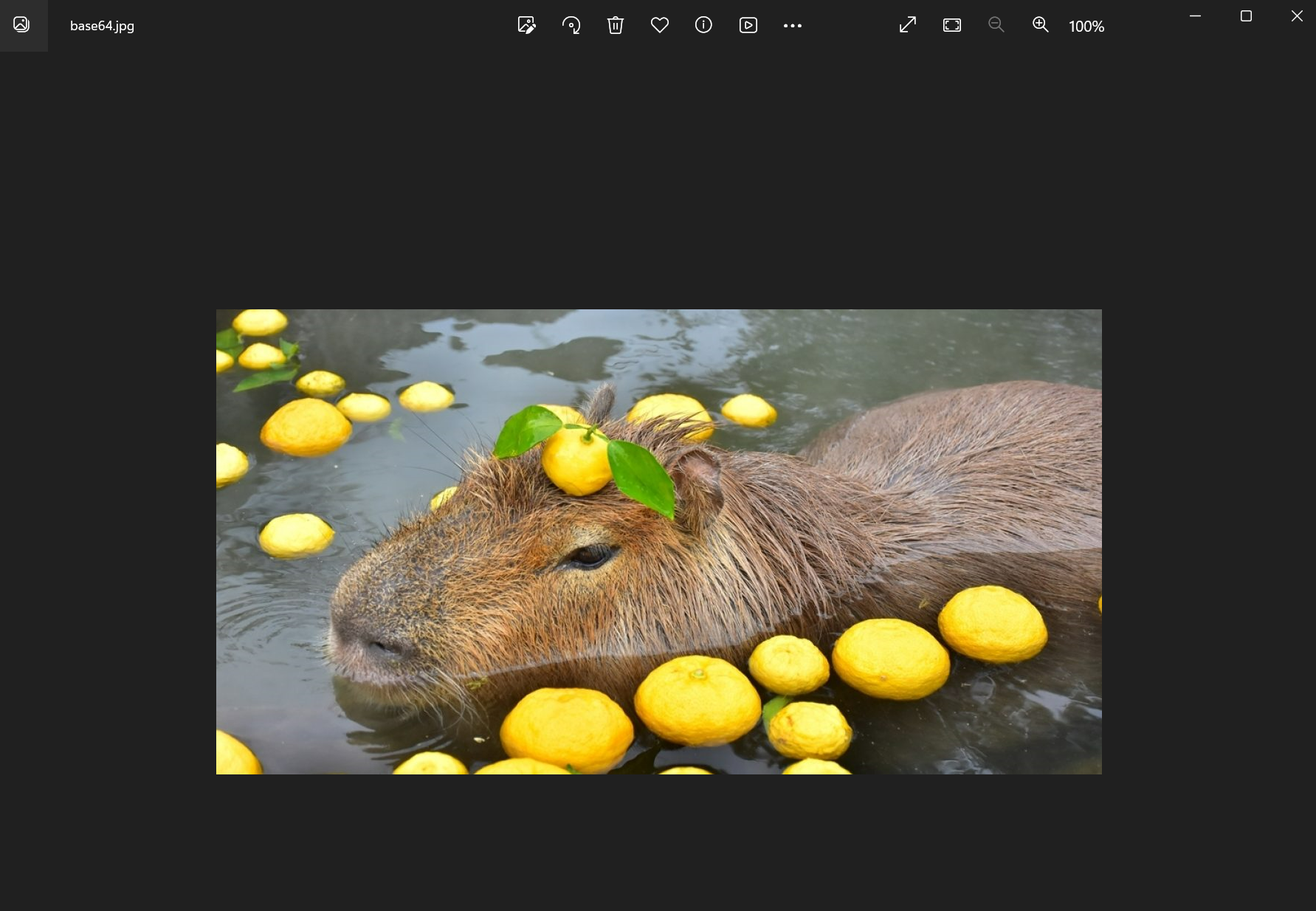
Description automatically generated

Hmm có vẻ như file vẫn không thể xem được. Mình nghĩ rằng đây chắc chắn là base64 encode rồi nhưng mà có thể format của nó chưa chuẩn nên không thể xem. Vì vậy mình quay lại trang analyze lúc nãy và dùng luôn format mà trang đề xuất.

A screenshot of a computer

Description automatically generated

Nhìn có vẻ okay rồi nên mình tải file decode xuống và đổi đuôi extension thành .jpg xem có mở được file không



Tada ta đã xem được hình ảnh bên trong rồi. Nhưng vấn đề là không có flag ở trong file ảnh này. Thời gian đang hết dần nên mình cắn răng dung hint nhưng mất 5 point ☹

A screenshot of a computer

Description automatically generated

Hint chỉ ra rằng đây không phải là một file ảnh. Mình nhận ra vấn đề và sử dụng hxd để kiểm tra file ảnh này

Mình kéo xuống end chunk thì nhận ra điều bất thường đó chính là file này có một file ảnh này chứa một file audio bên trong

A screenshot of a computer code

Description automatically generated

Sai lầm của mình ở bài này chính là không đọc kỹ đề. Đề ở đây chỉ yêu cầu nhập flag là tên file bị ẩn và ở đấy chính là file audio.wav nhưng mình vẫn tiếp tục mở file audio.wav lên

A screenshot of a black screen

Description automatically generated

Đây là một file âm thanh chứa mã morse dài 1 phút và mình ngay lập tức up lên trang web decode mã morse online và thu được một đoạn text : EL04354467B64305F7930555F6B4E3057575F6830575F74305F52334445F6D307235335F433064333F7D

Ném lên CyberChef thì không decode ra được gì cả cho nên mình đã bỏ qua bài này mặc dù flag đã rõ mồn một rồi ☹Về nhà ngẫm ra thì đã quá trễ rồi

Flag : EHC{audio.wav}