LAB 01

Thầy Mai Hoàng Đỉnh
Trường đại học FPT

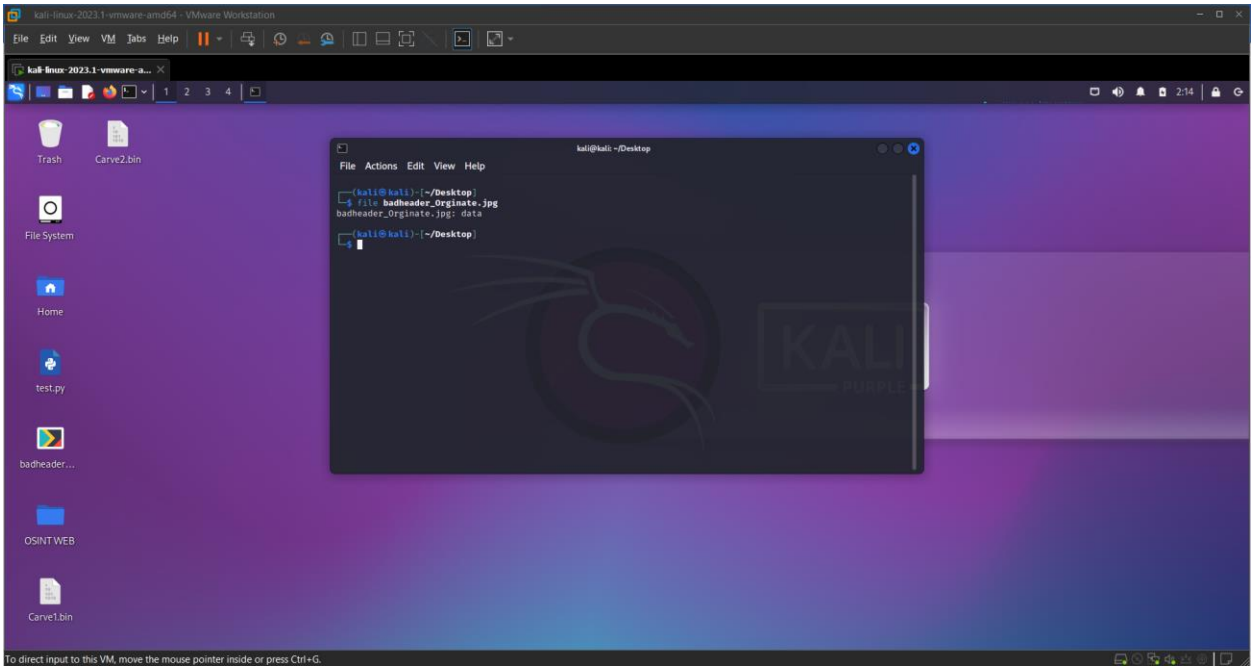
Người thực hiện

Đặng Hoàng Nguyên

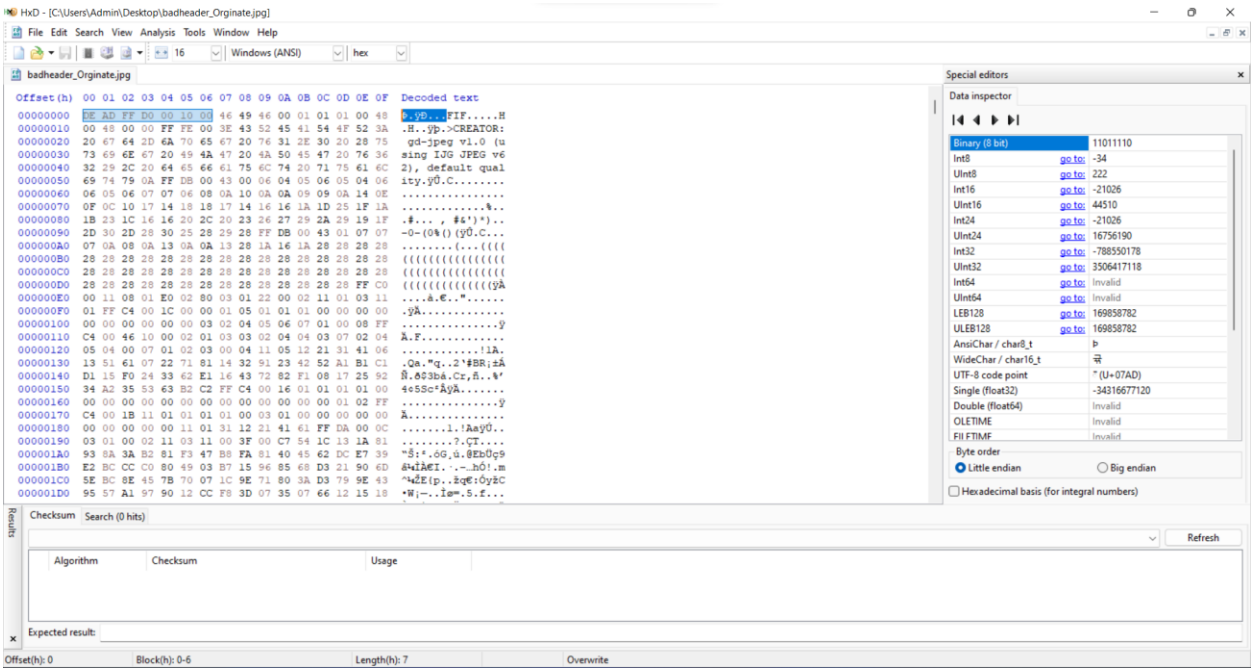
Lab 1: Preparing a Virtual Windows Machine

badheader_Orginate.jpg

Chúng ta sẽ sử dụng command **file <filename>** để có thể xem được file đó hiện đanng là file gì

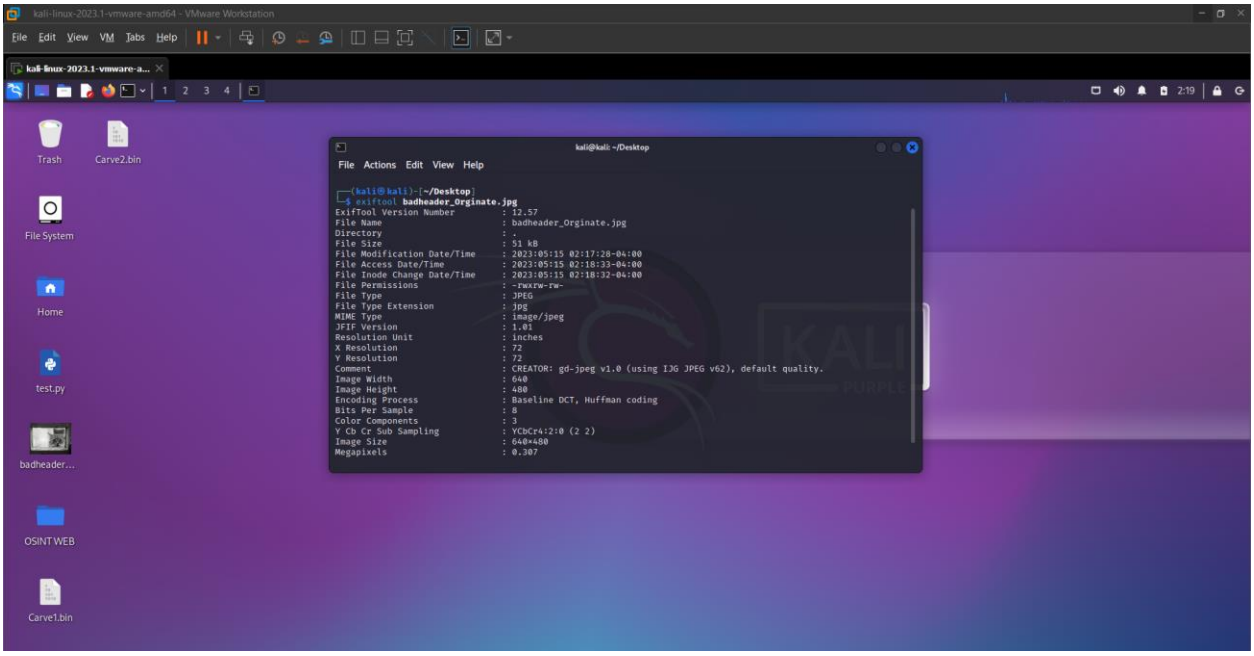


Dùng các công cụ như HXD, Bless hay hexeditor để có thể xem hex của chúng



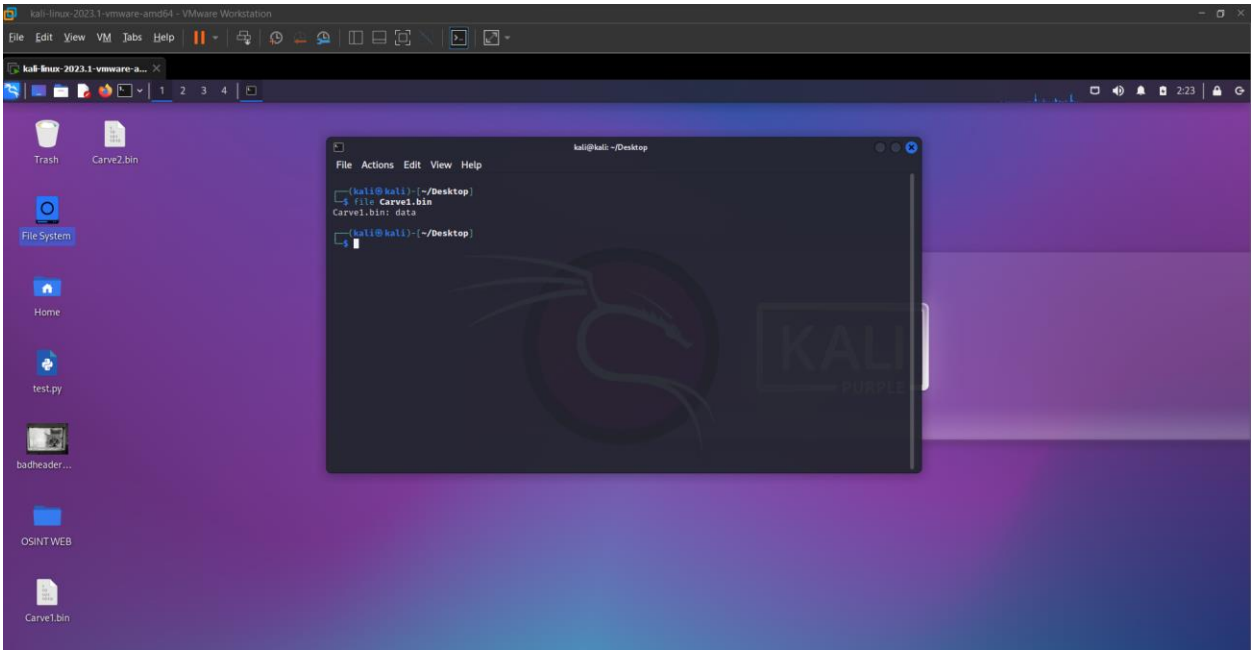
Có vẻ như là Magic Header của file đã bị thay đổi. Chúng thay đổi từ DE AD FF D0 00 10 00 46 49 46 ta sẽ chuyển lại sang FF D8 FF E0 00 10 4A 46 49 46 00 01. Và sau đây là kết quả

Kiểm tra metadata bằng **exiftool** ta có thể thấy nó chính là file jpeg



Carve1.bin

Đây đang hiện tại là file có đuôi .bin là một file binary nhưng khi check bằng command find, ta có thể thấy rằng đây không phải là file binary. Đây là một file không xác định nên nó mới để dạng file type là data.

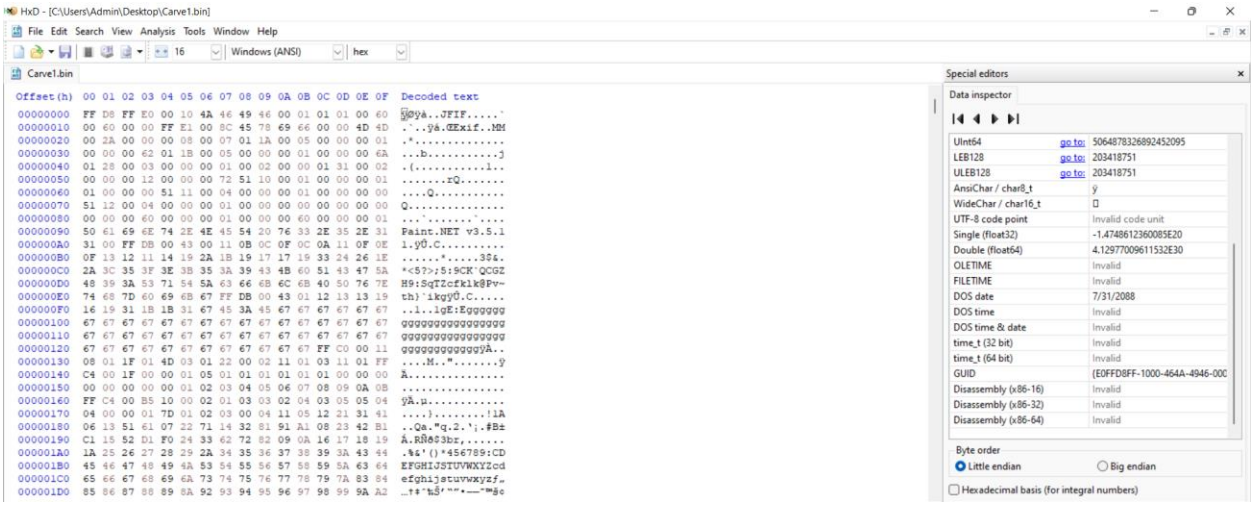


Kiểm tra bằng công cụ hxd để kiểm tra, thì đúng là các byte đầu của offset đều được chỉnh về 00. Nếu chúng ta kiểm tra offset 1250 ta có thể thấy rằng ở đây có bắt đầu header của JPEG

```
00001240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001250  00 00 00 00 00 00 00 00 FF D8 FF E0 00 10 4A 46  ............ÿØÿà..JF
00001260  49 46 00 01 01 01 00 60 00 60 00 00 FF E1 00 8C  IF.....`.`..ÿá.Œ
00001270  45 78 69 66 00 00 4D 4D 00 2A 00 00 00 08 00 07  Exif..MM.*......
00001280  01 1A 00 05 00 00 00 01 00 00 00 62 01 1B 00 05  ...........b....
00001290  00 00 00 01 00 00 00 6A 01 28 00 03 00 00 00 01  .......j.(......
000012A0  00 02 00 00 01 31 00 02 00 00 00 12 00 00 00 72  .....1.........r
000012B0  51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04  Q...........Q...
000012C0  00 00 00 01 00 00 00 00 51 12 00 04 00 00 00 01  ........Q.......
000012D0  00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 01  ...........`....
000012E0  00 00 00 60 00 00 00 01 50 61 69 6E 74 2E 4E 45  ...`....Paint.NE
000012F0  54 20 76 33 2E 35 2E 31 31 00 FF DB 00 43 00 11  T v3.5.11.ÿÛ.C..
00001300  0B 0C 0F 0C 0A 11 0F 0E 0F 13 12 11 14 19 2A 1B  ..............*.
00001310  19 17 17 19 33 24 26 1E 2A 3C 35 3F 3E 3B 35 3A  ....3$&.*<5?>;5:
```

FF D8 FF DB	ÿØÿÛ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format[14]
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà‰‰JFIF‰‰			
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá??Exif‰‰			
FF D8 FF E0	ÿØÿà	0	jpg	JPEG raw or in the JFIF or Exif file format[14]

Bây giờ chúng ta chỉ việc xóa các byte 00 trước đó, lưu file extension dưới dạng .jpg thì ta có thể xem được file

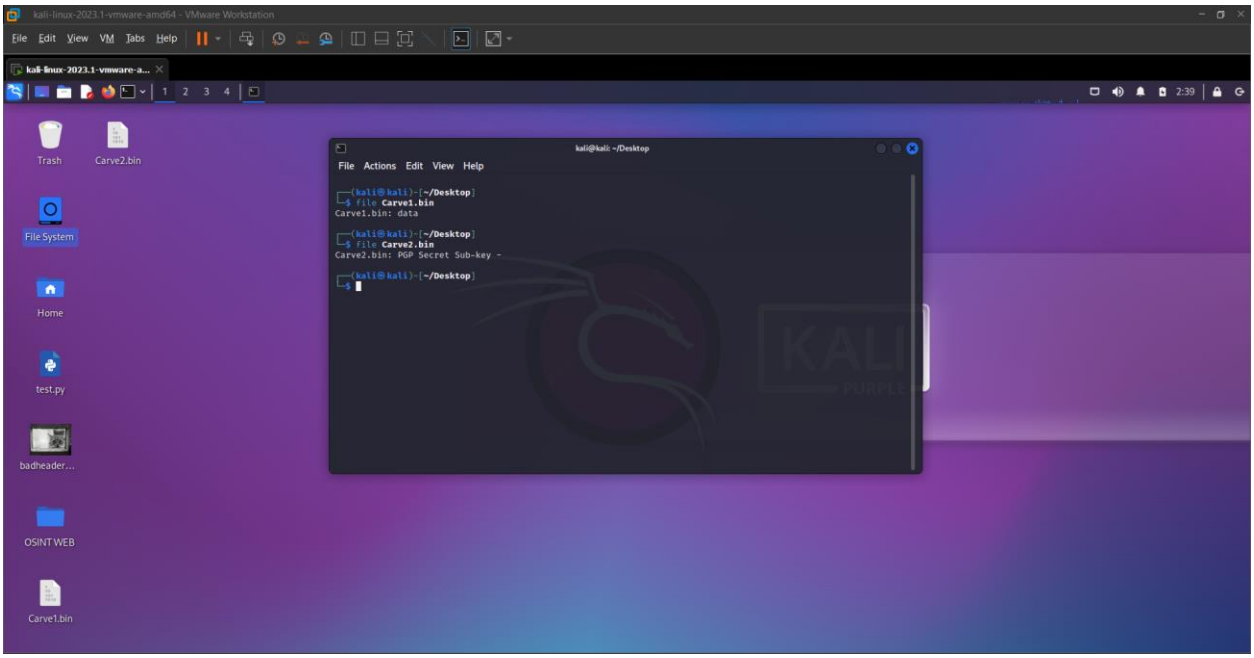


Ctrl + S và lưu lại dưới dạng Carve.jpg

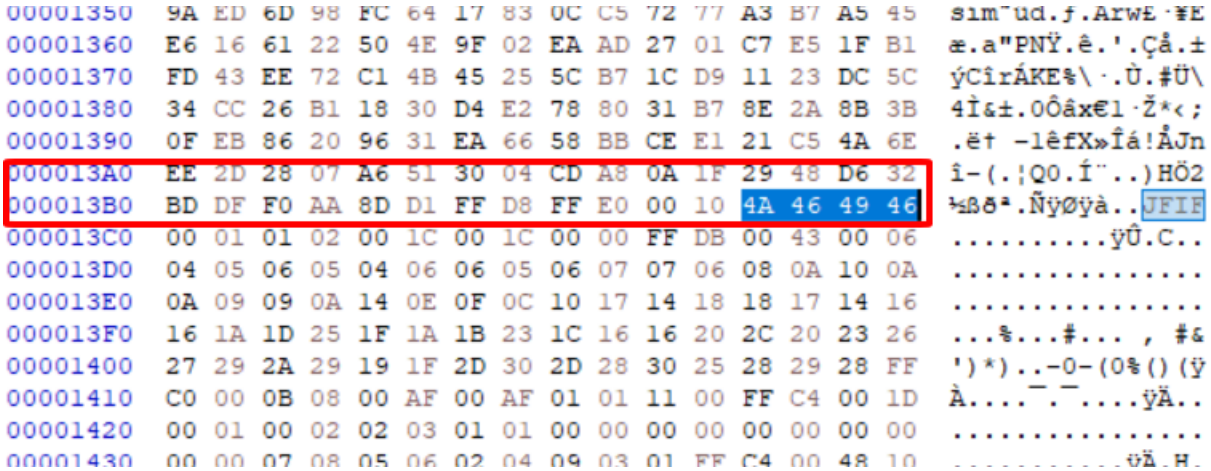
Và ta có thể mở được file

Carve2.bin

Như thường lệ, ta sẽ bỏ nó vào trong kali và check với câu lệnh **file** để xem đọc header nó đọc những gì



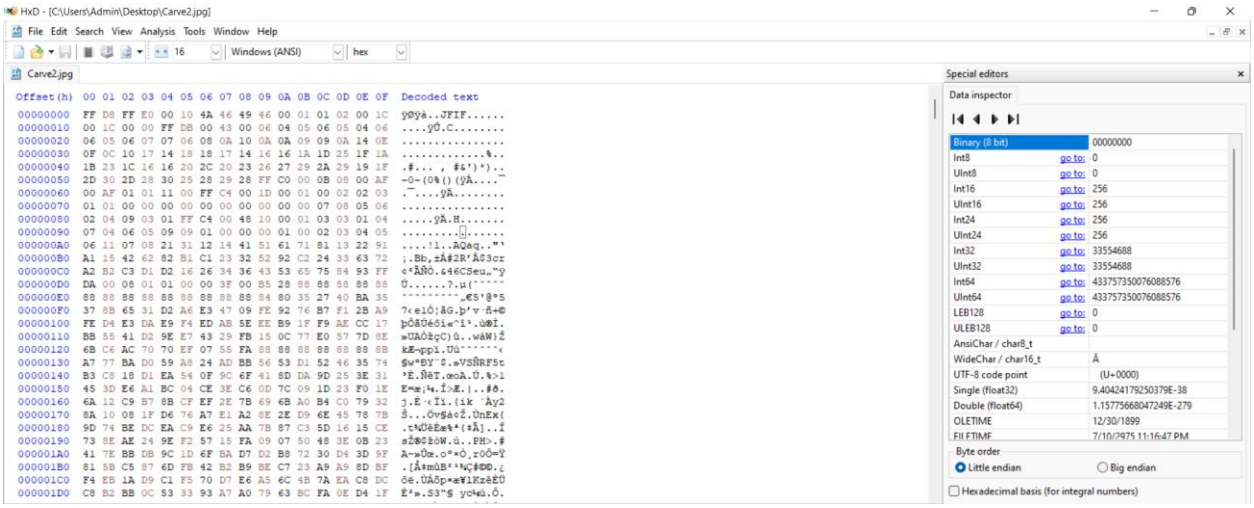
Theo như dự định ban đầu thì Carve2.bin nó là một file key PGP. Nhưng nếu bỏ vào HXD để kiểm tra thử, ta có thể thấy rằng file ngoài là một file key PGP, thì nó có phần Offset chứa một file JPEG. Vào HXD sử dụng tổ hợp **Ctrl + F** và search string **JFIF** hoặc có thể sử dụng Hex value và tra cứu **FF D8 FF E0 00 10 4A 46 49 46 00 01**.



Tại phần OFFSET 13B0 ta có thể tìm được header của file JPEG. Việc của chúng ta cần làm là lấy file JPEG đó ra để xem hình đó là gì. Có hai cách trong trường hợp này:

Cách 1:

- Copy từ đoạn header FF D8 trở xuống, và sử dụng một tab mới trong HXD bằng cách sử dụng tổ hợp **ctrl N,** sau khi bật tab mới, ta chỉ việc copy đoạn max hex của nó và save thành một file mới.



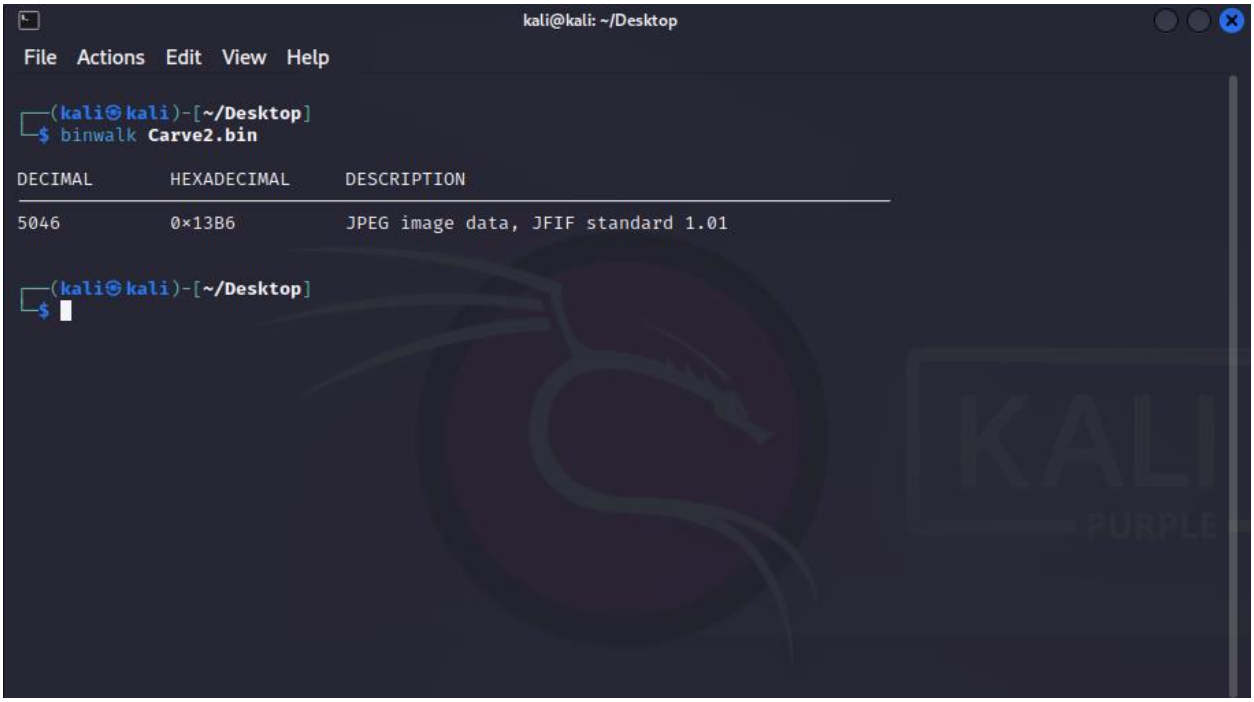
Đây là file mới chúng ta đã copy ra rồi. Save lại dưới đuôi file là JPG chúng ta sẽ ra được file cần đọc

Cách 2:

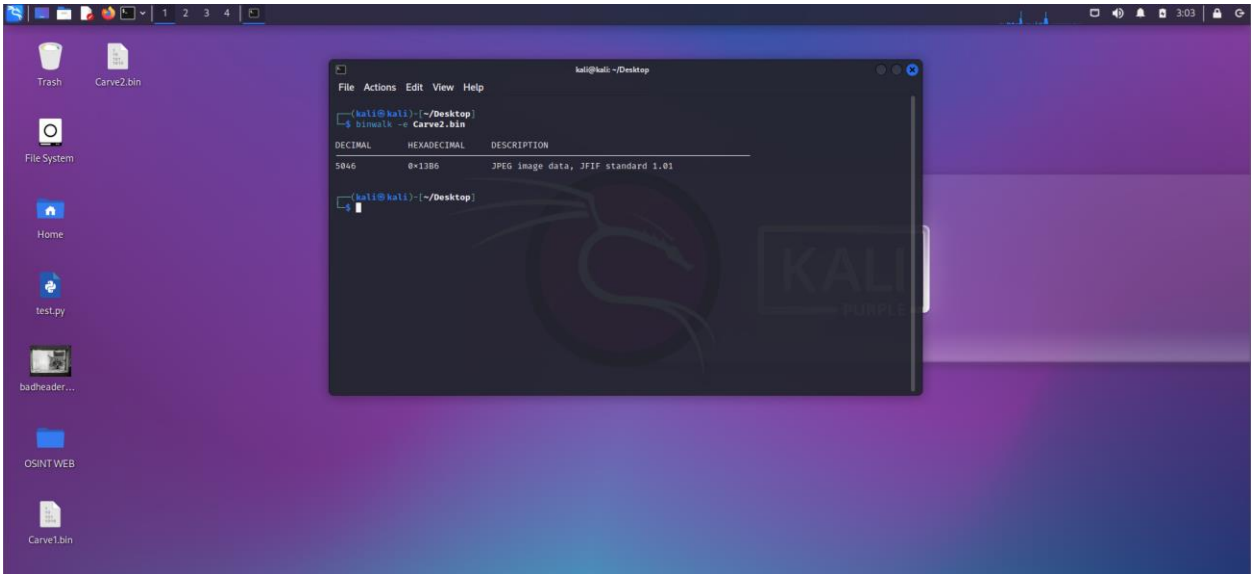
- Xóa đoạn PGP key ở đằng trên, nhưng như thế sẽ làm hư file bằng chứng.

Ngoài 2 cách trên, chúng ta có thể extract hình ra một cách dễ dàng mà không cần phải sử dụng tới HXD, đó chính là sử dụng công cụ binwalk trên kali. Binwalk cho chúng ta có khả năng xem được những file bị embedded trong một file khác.

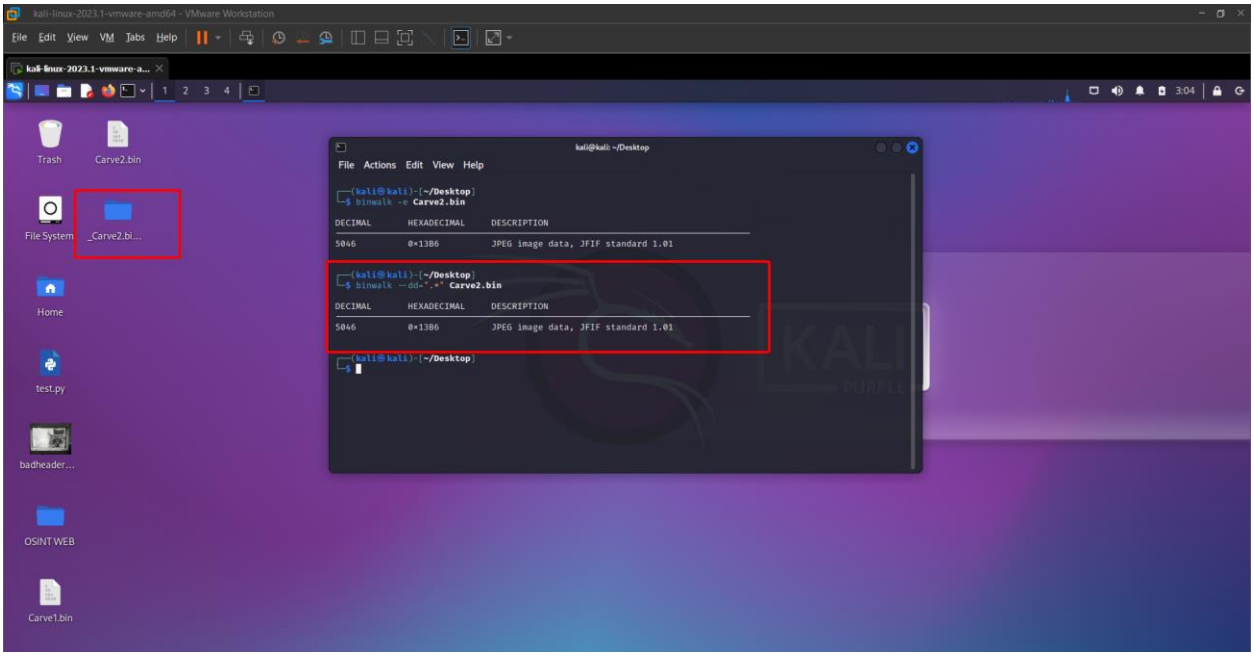
B1: Check bằng command **binwalk <filename>**



B2: Sử dụng command **binwalk -e <filename>** để extract file hình ra. Sau đó nó được lưu vào folder _Carve2.bin



Nhận thấy rằng khi dung command **binwalk -e** Carve2.bin không ra được folder _Carve2.bin, ta sử dụng lệnh sau để ép extract tất cả các embedded file: **binwalk –d=".*" <filename>**



Ta thấy rằng tại đây đã xuất hiện folder _Carve2.bin. Vào đó và mở file lên thì ta có được hình sau: