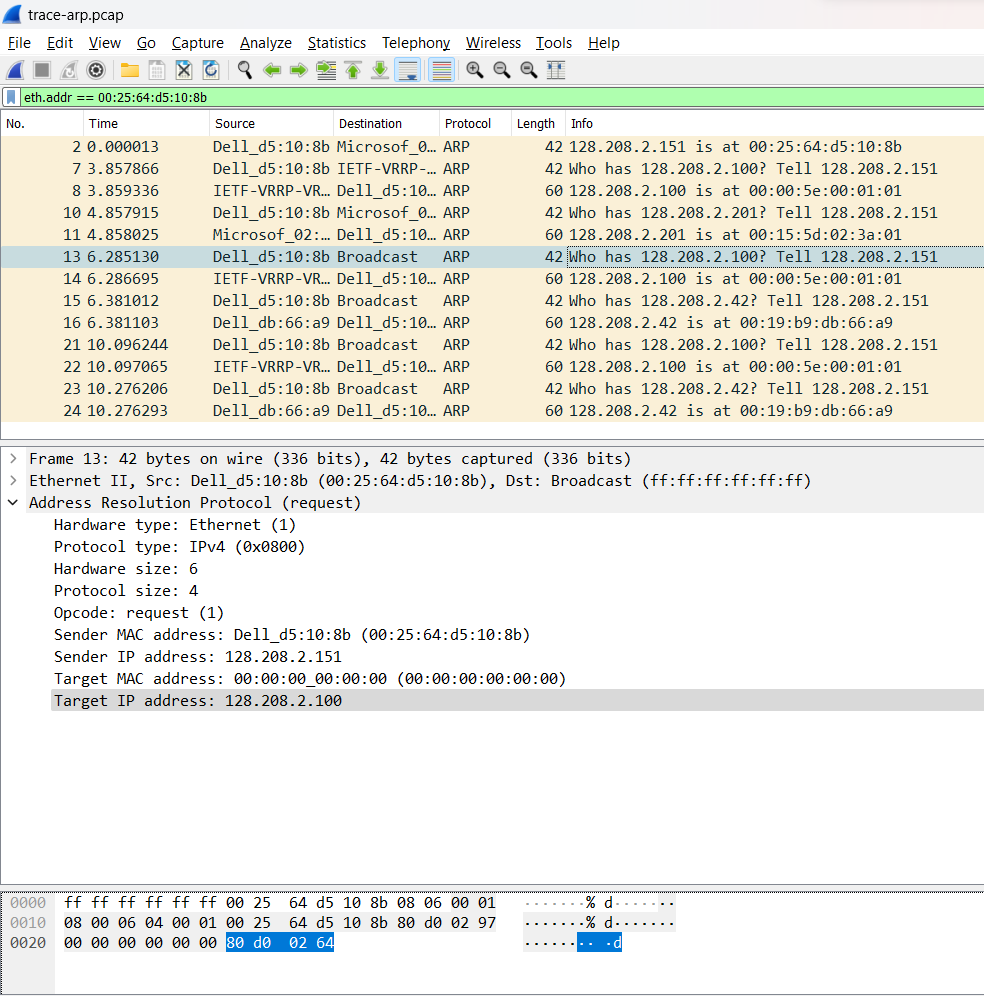
# LAB 1.1: ARP



1. Opcode

* Request: 1
* Reply: 2

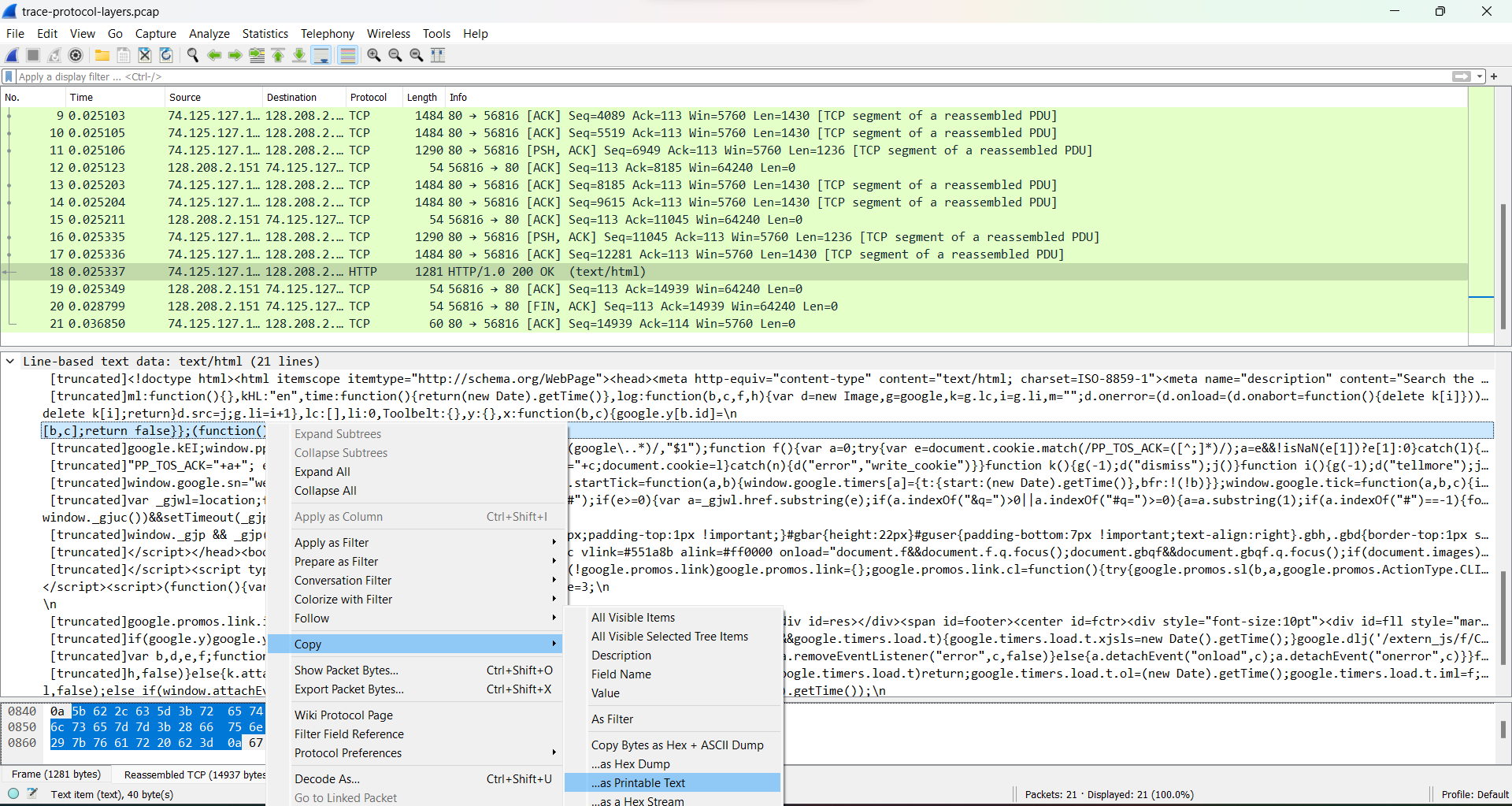
2. 28 byte cho cả header ARP request và reply

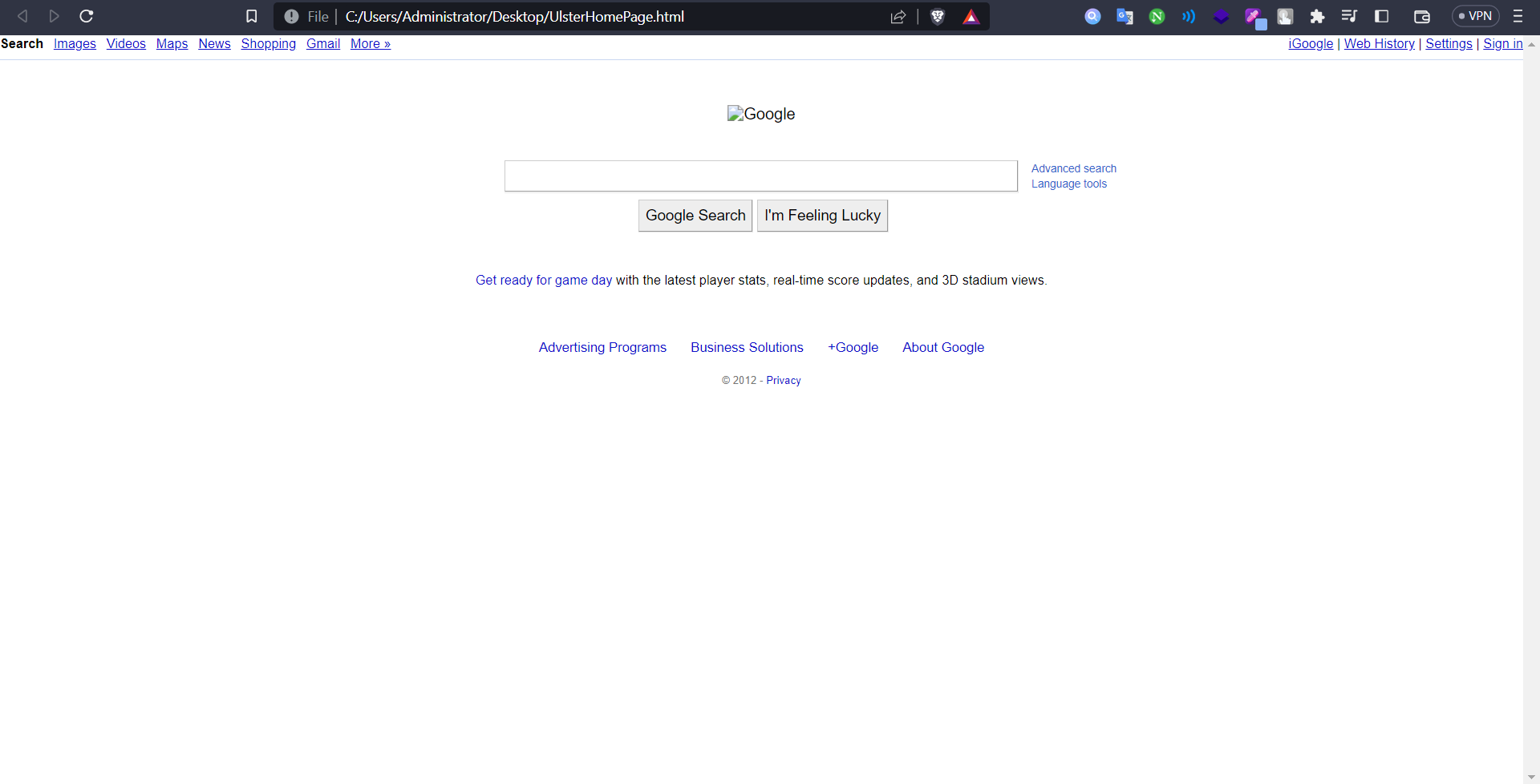
3. 00:00:00:00:00:00

4. 0x806

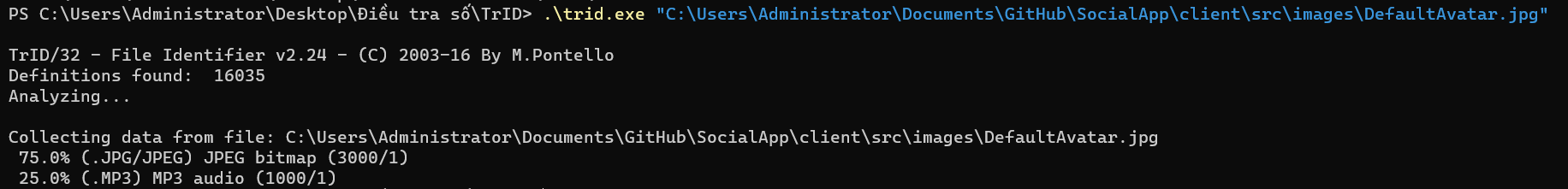
5. Không. Nó được gửi trực tiếp đến mục tiêu bằng địa chỉ Ethernet của nó.

# LAB 1.2 : PROTOCOL LAYERS

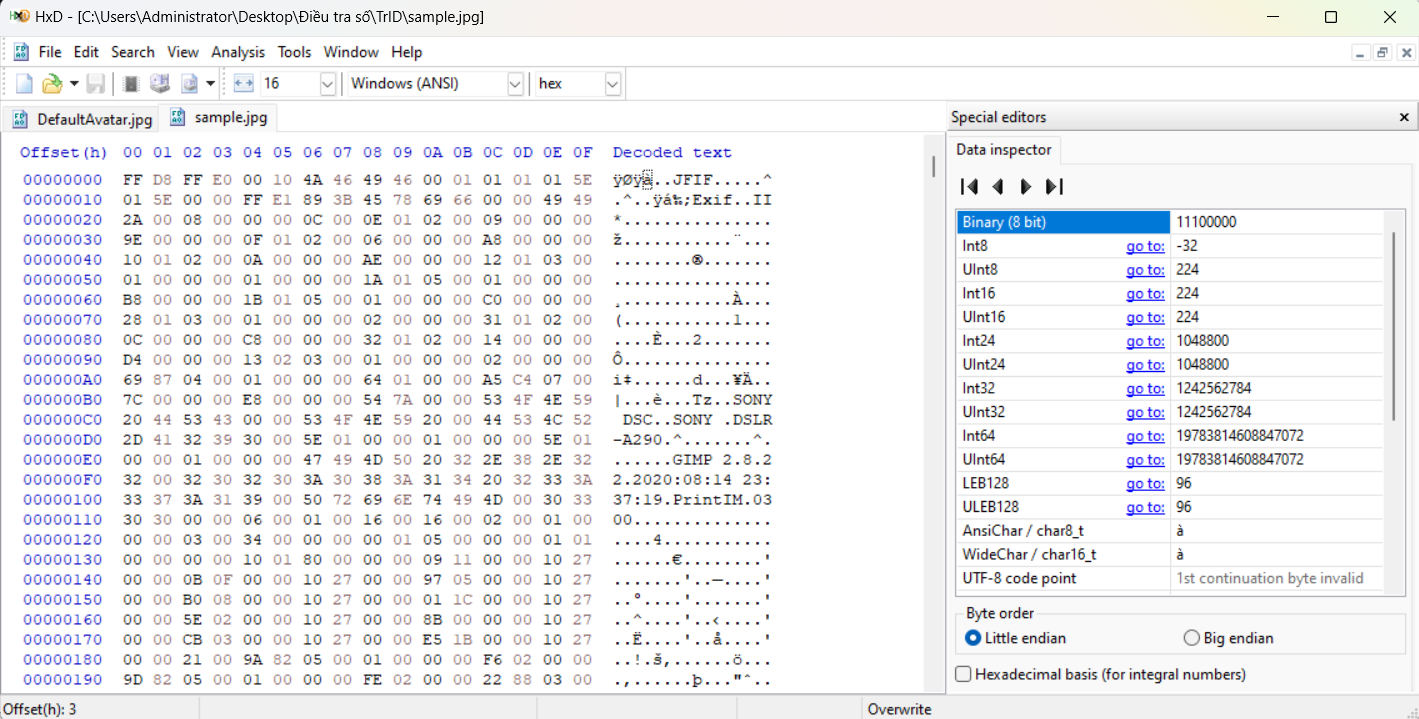




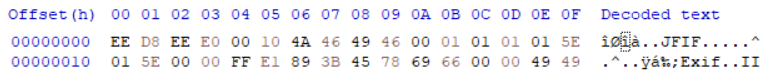
**1. Using HexView to view header about JPEG, EXE to understanding FILE HEADER**



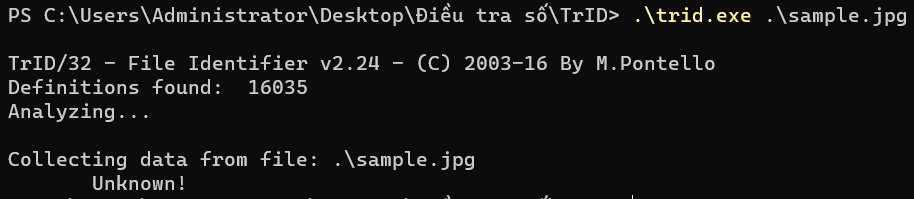
**View header JPEG by HexView**



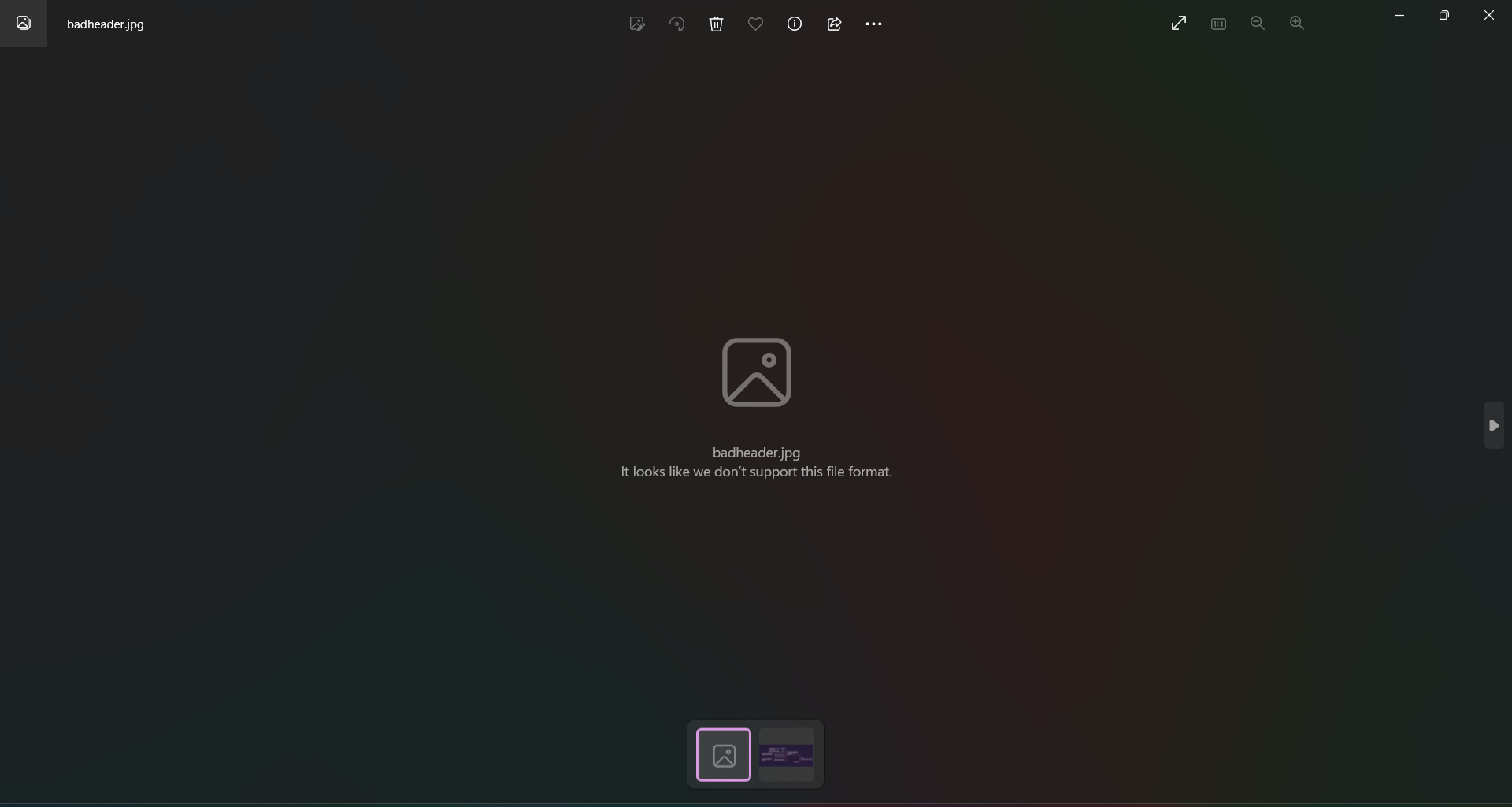
**Mofify FF-D8-FF-E0 to EE-D8-EE-E0 you can not see the picture.**

****

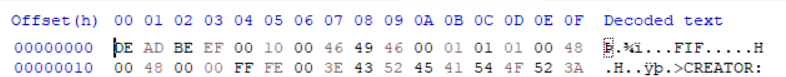
**Trid can not identify the flag file**



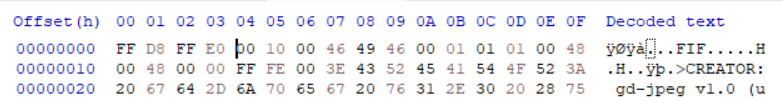
**2. Rebuilding an Image Header**



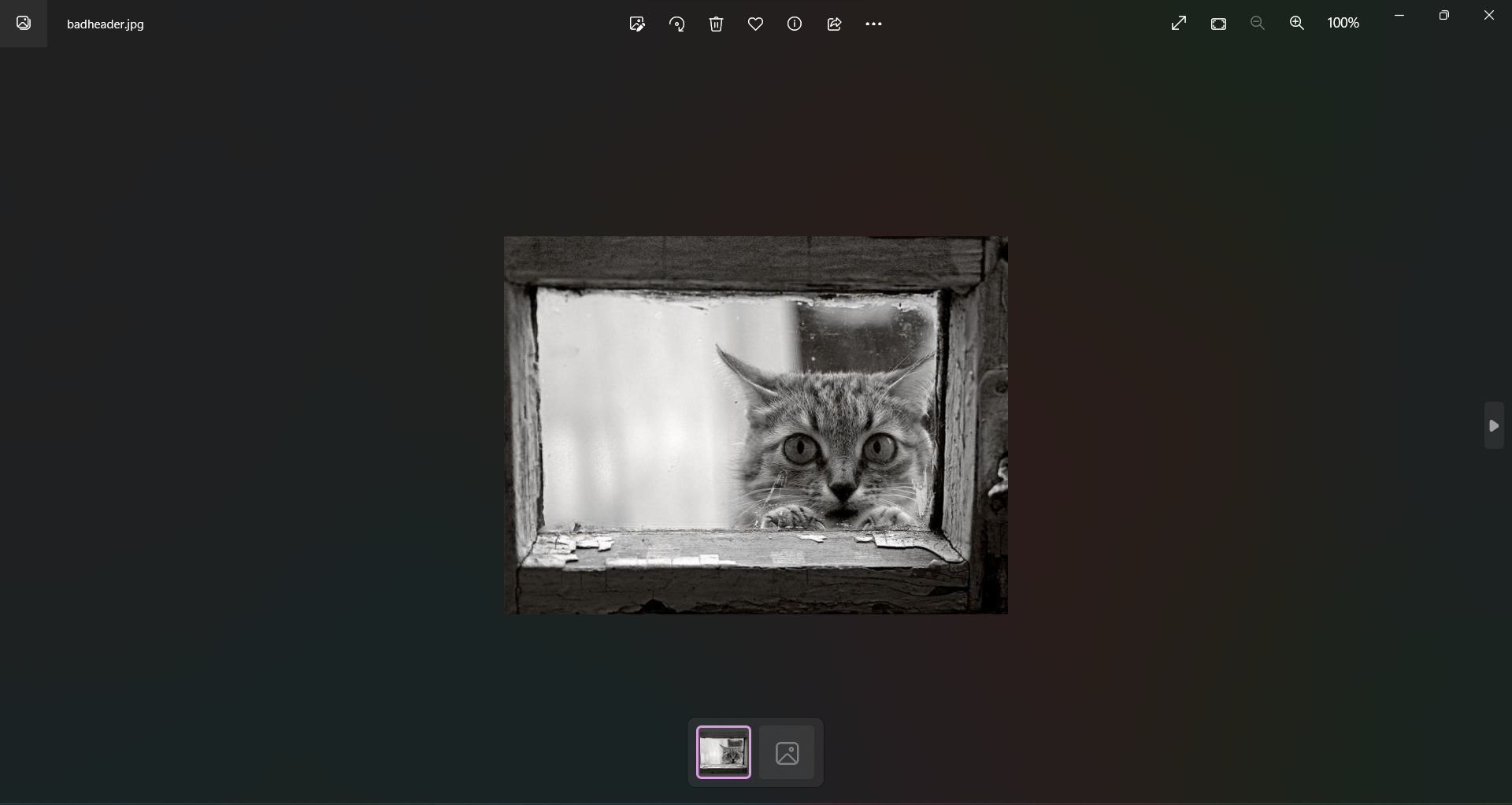
Không hiển thị được ảnh



Sau khi sửa lại header:



Ảnh sau khi khôi phục header:

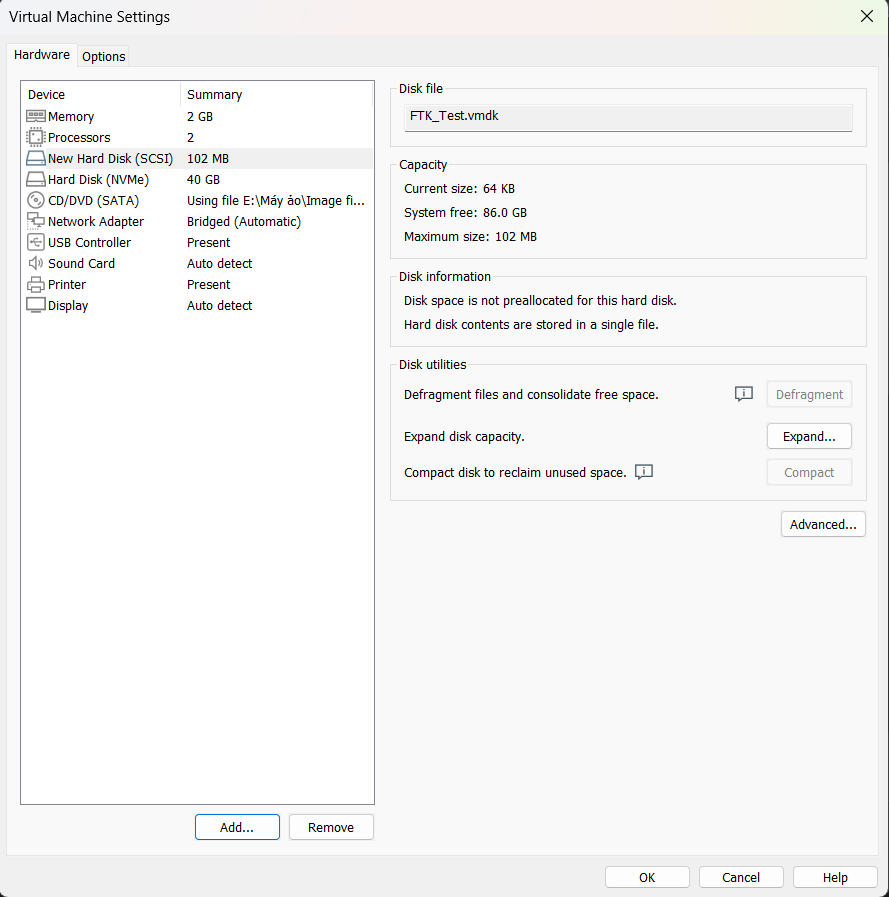


# LAB 2

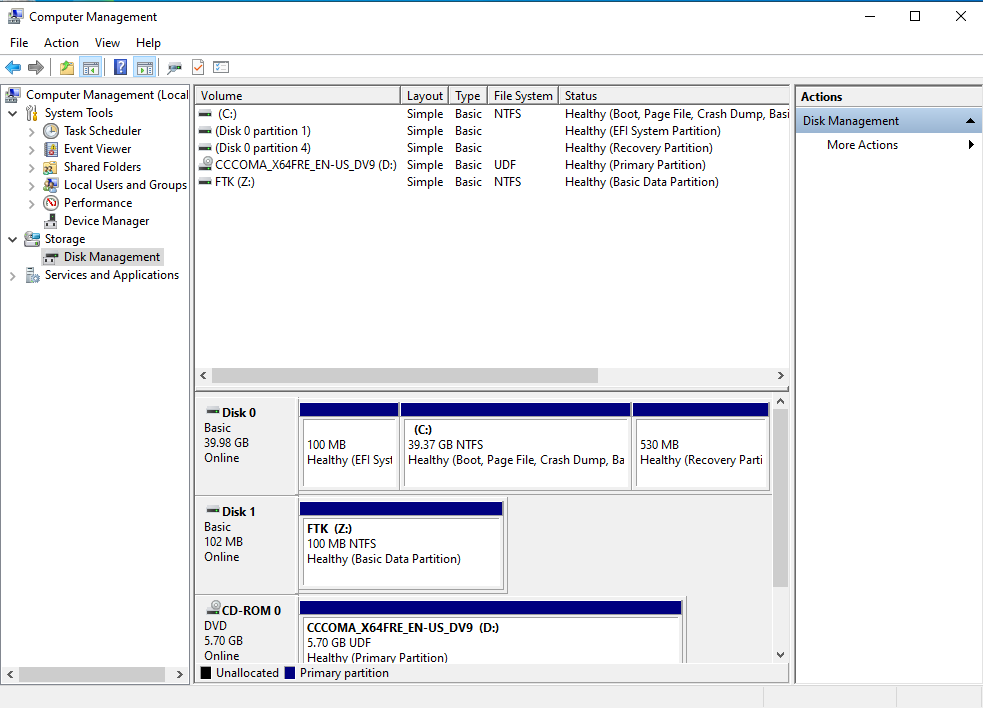


# LAB 3

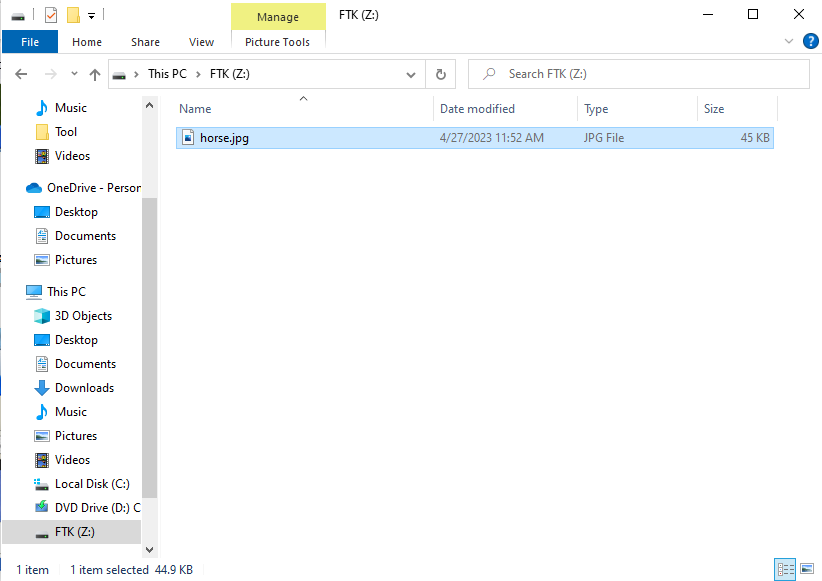
**Create new Hard Disk named FTK\_Test.vmdk**



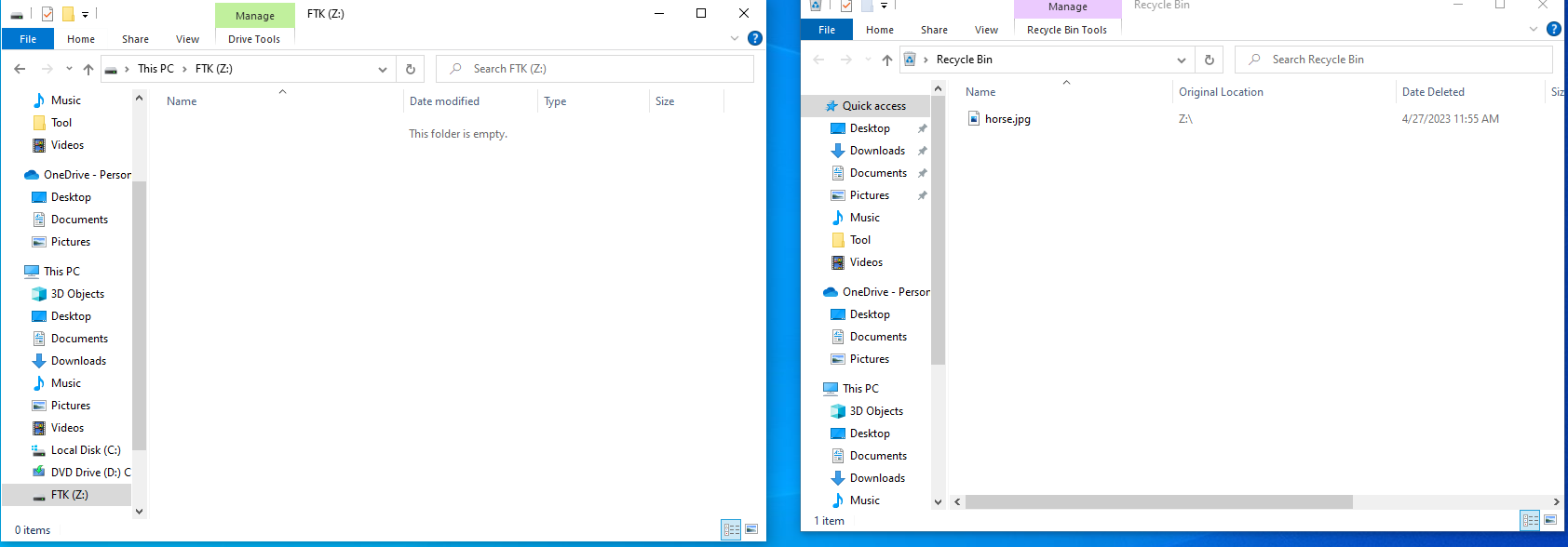
**Modify new Disk**

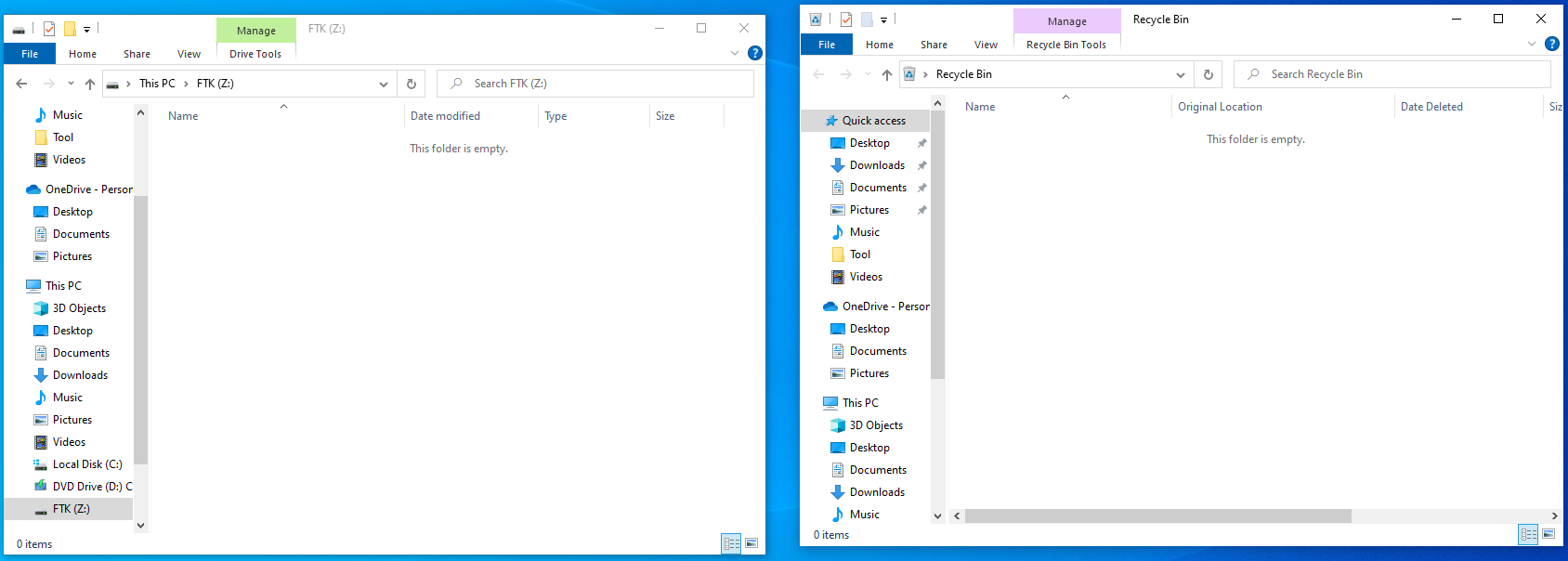


**Save Test Image in new FTK Disk.**

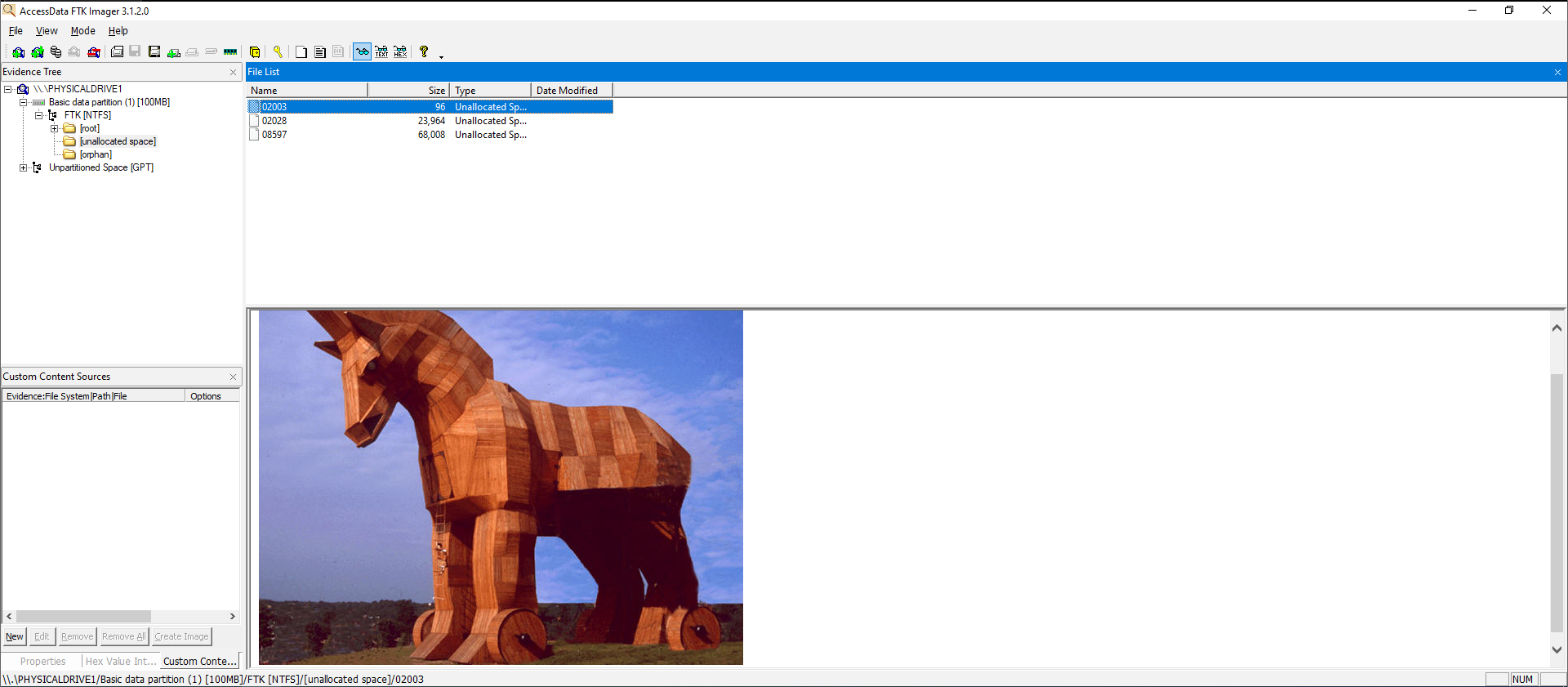


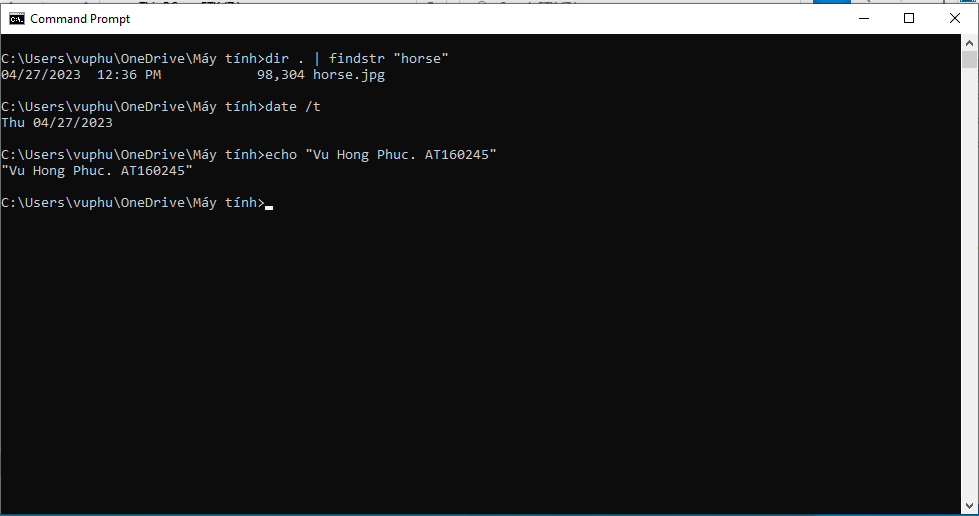
**Delete Test Image in FTK Disk and Recycle Bin**





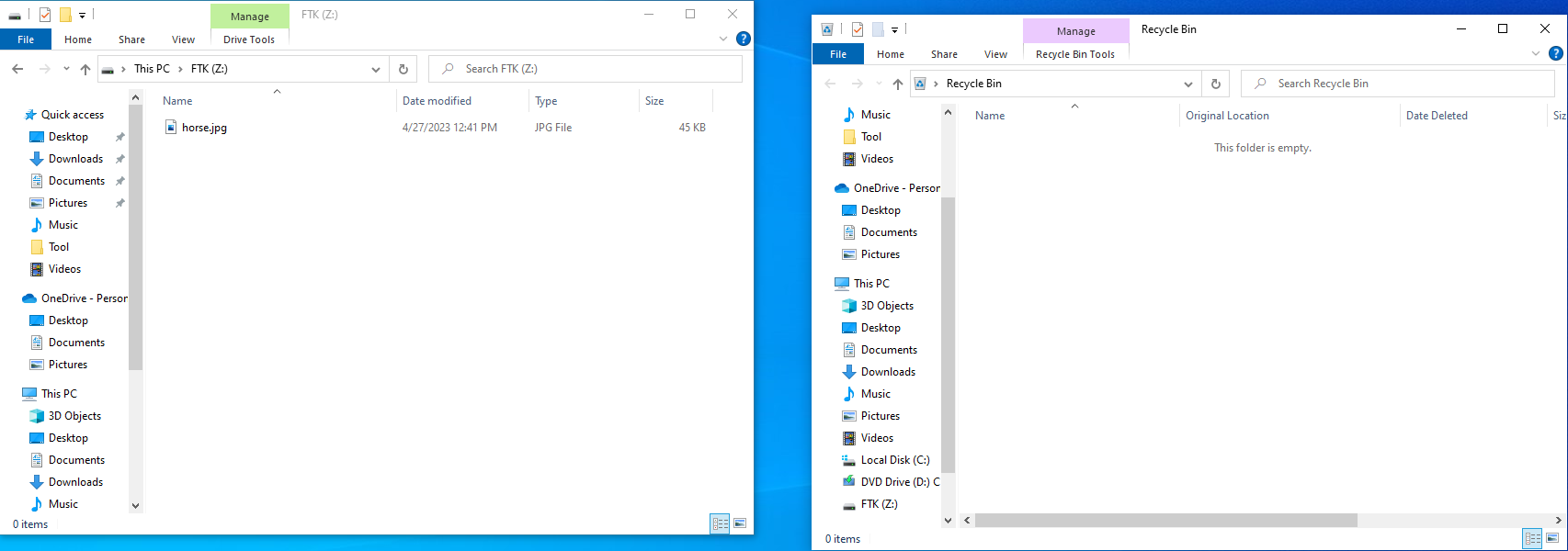
**Open FTK Imager and restore Image**



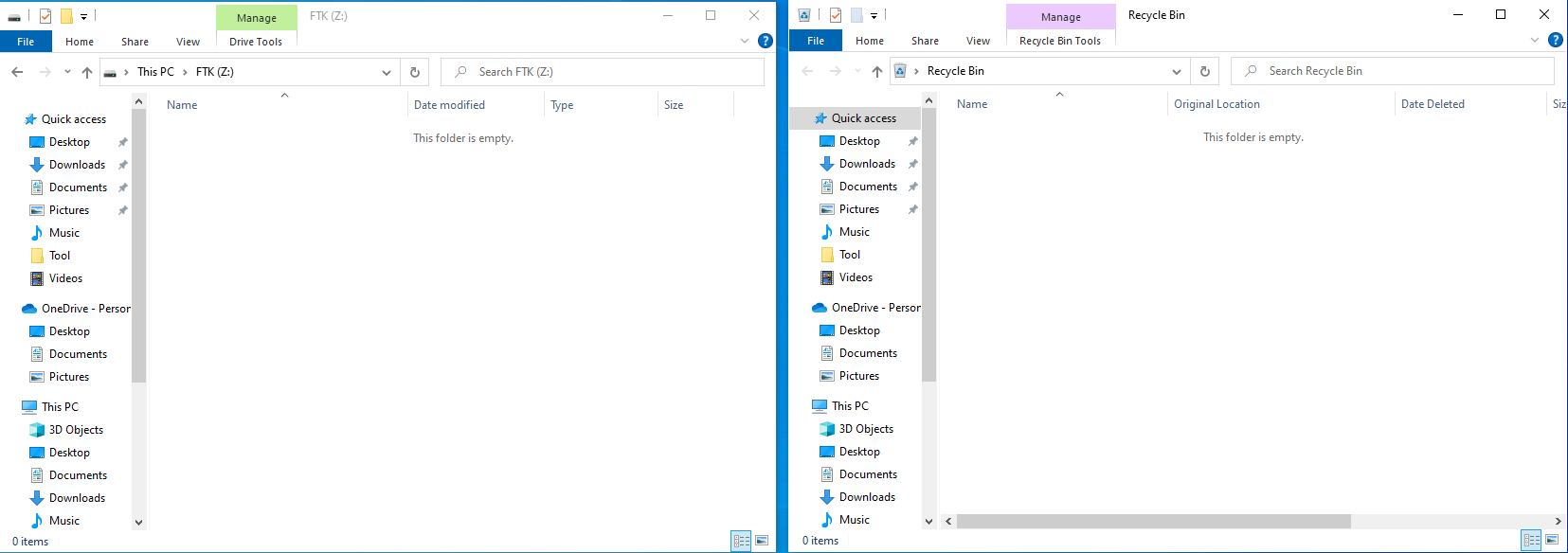


# LAB 4

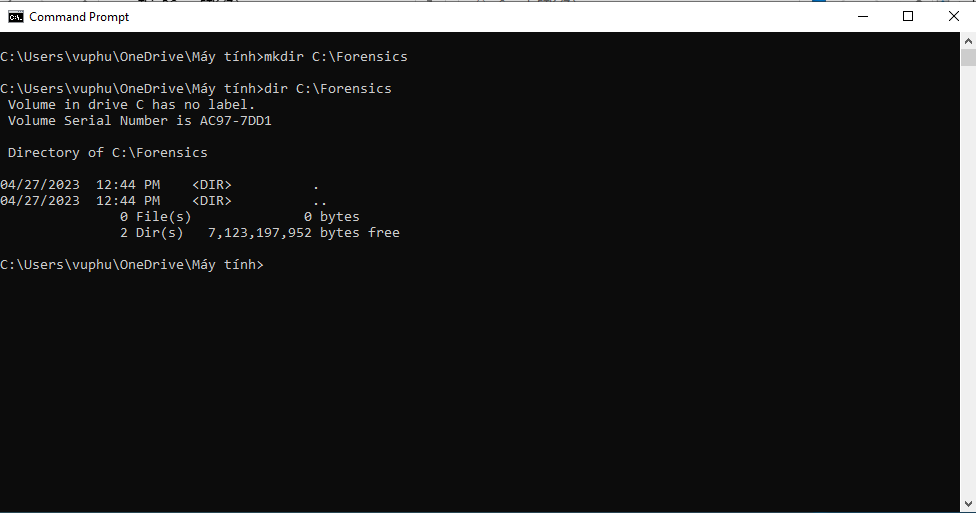
**Download Image to FTK Disk**



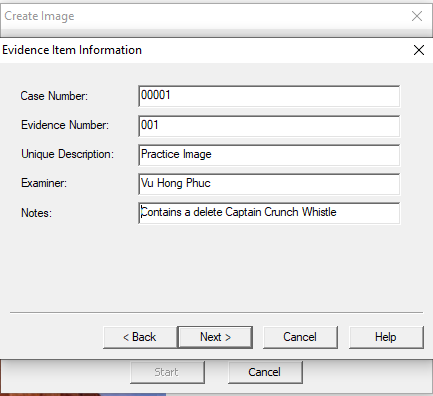
**Delete it from FTK Disk and Recycle Bin**

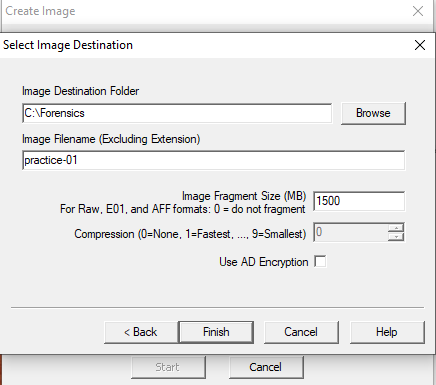


**Create new folder named Forensics on Disk C:**

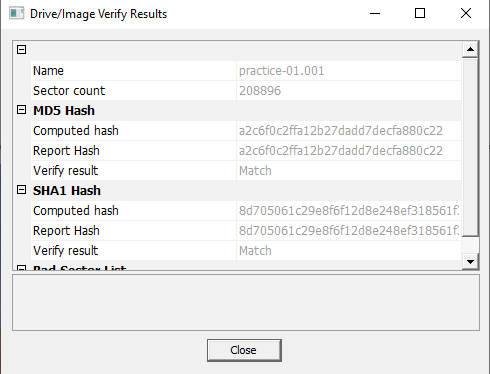


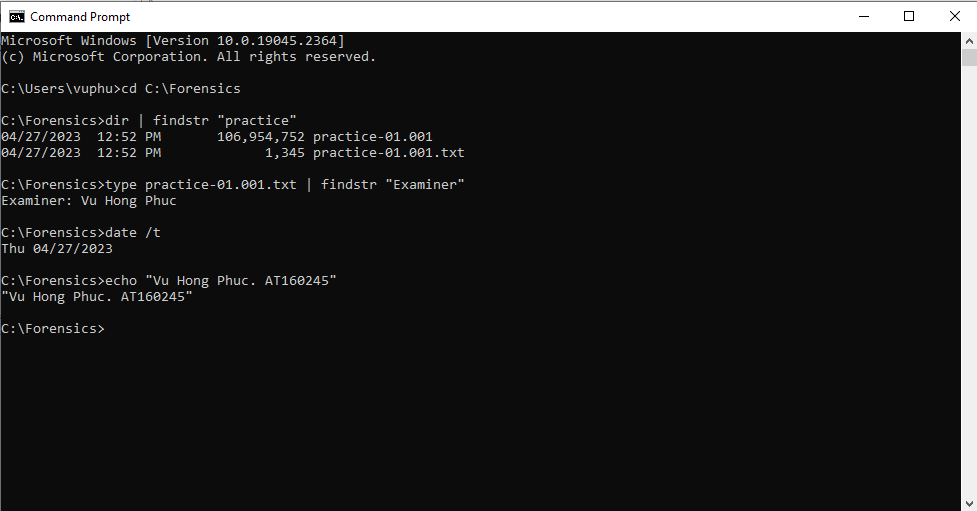
**Create Desk Image**





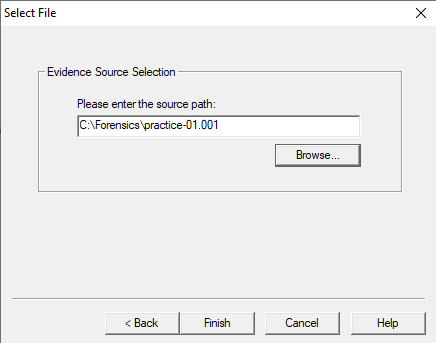
**Drive/Image Verify Results**



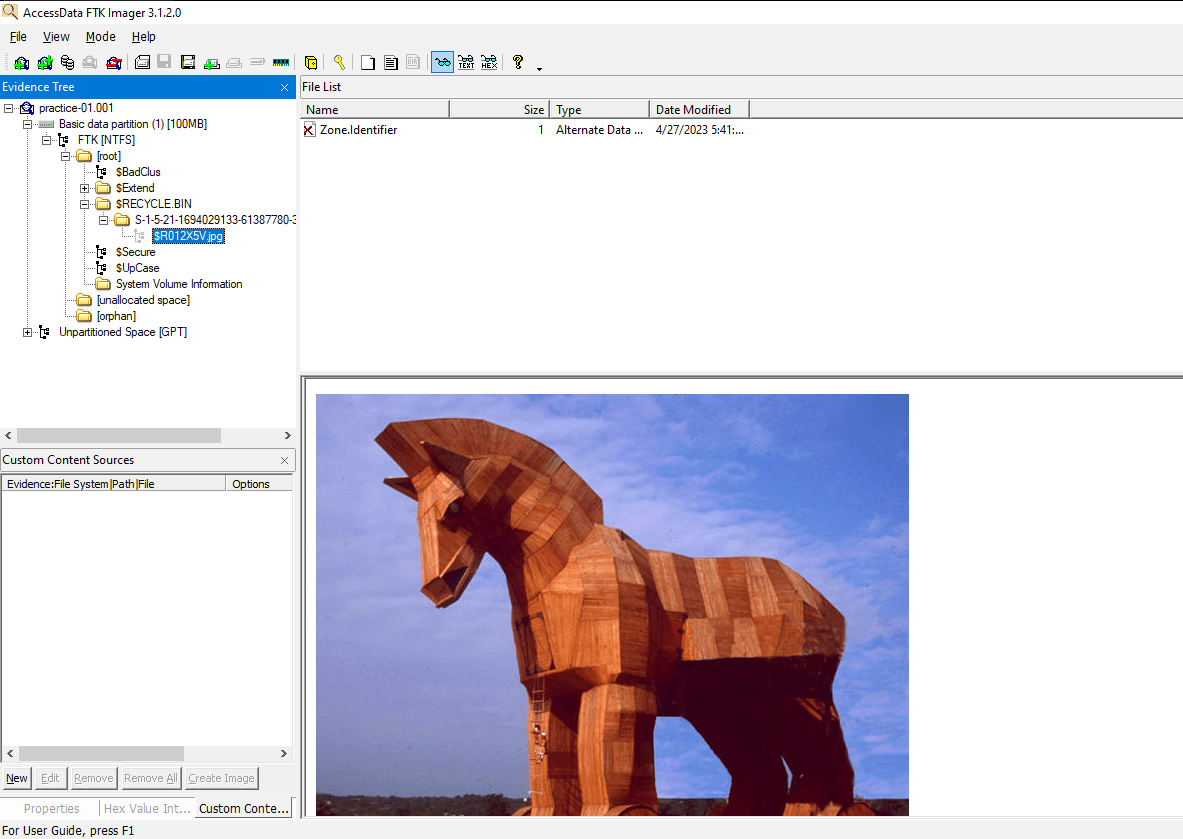


# LAB 5

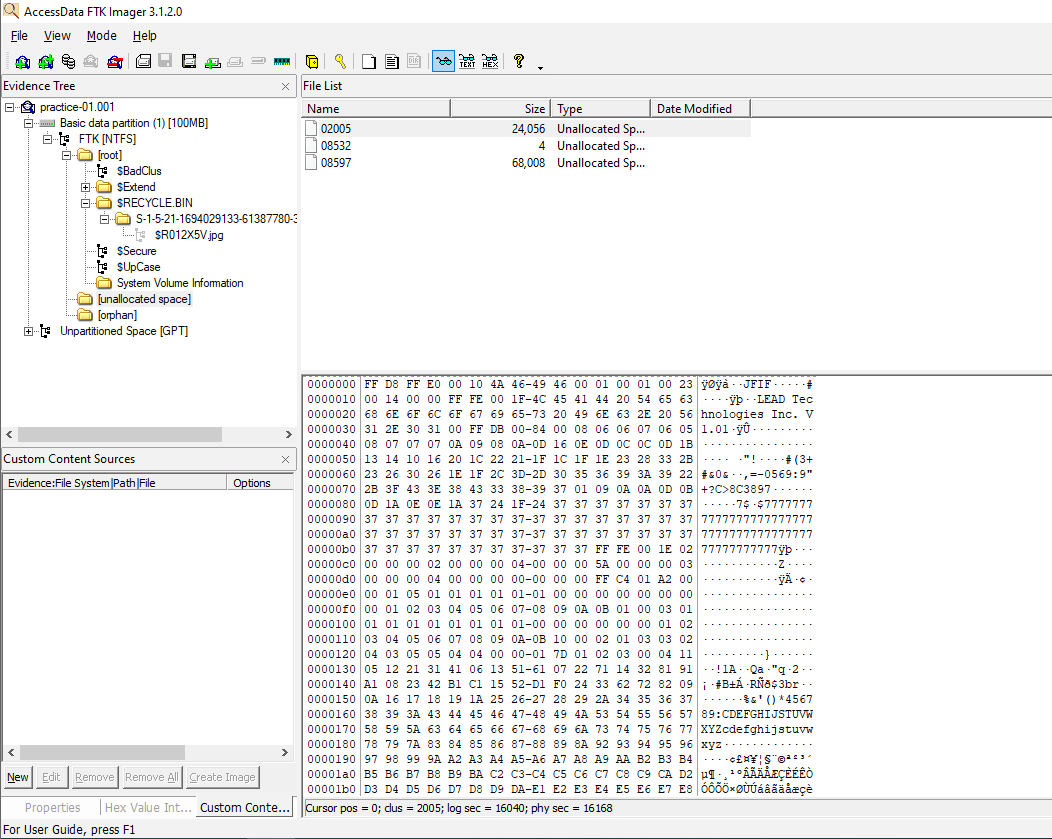
**Select file**



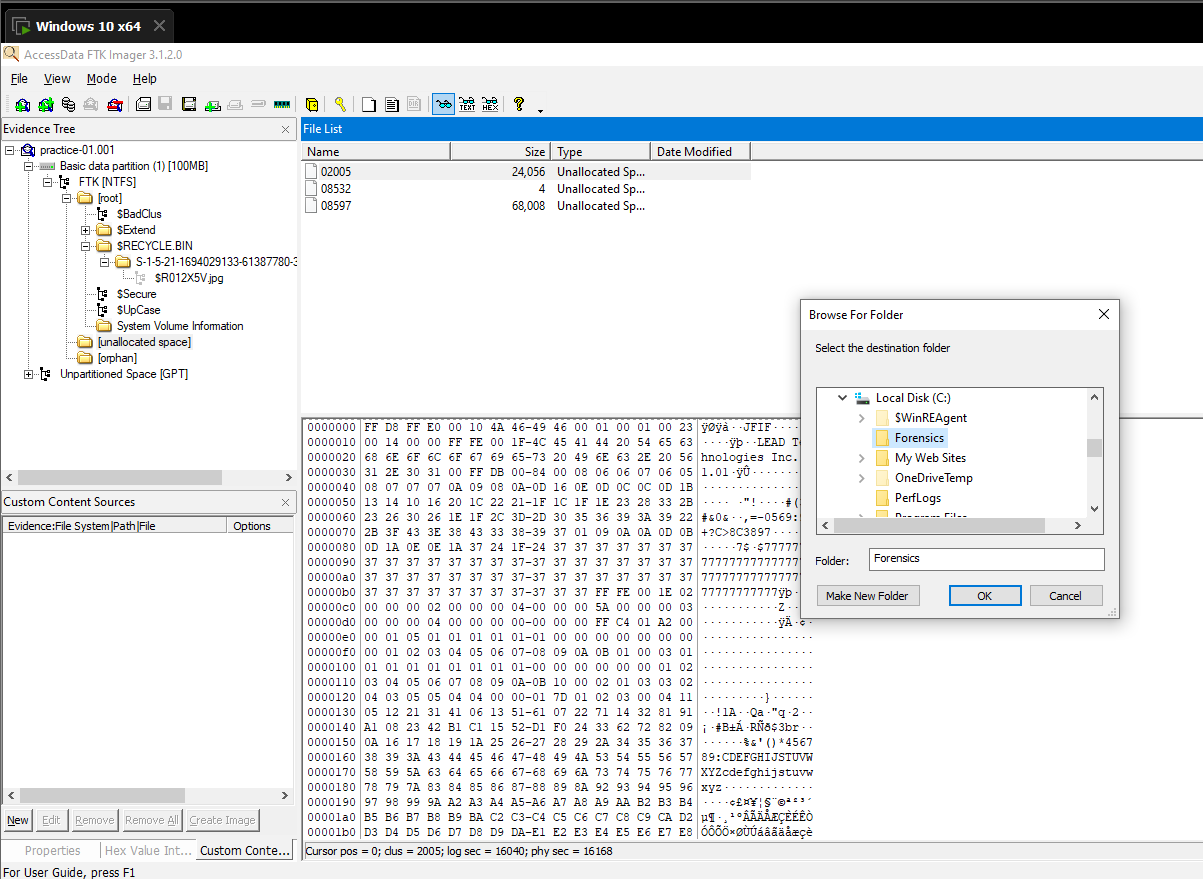
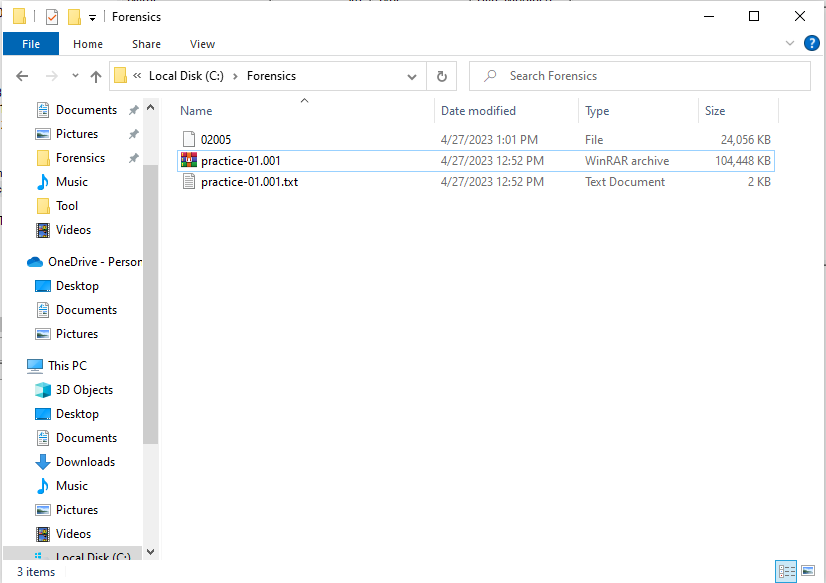
**View deleted file(s) in Recycle Bin**

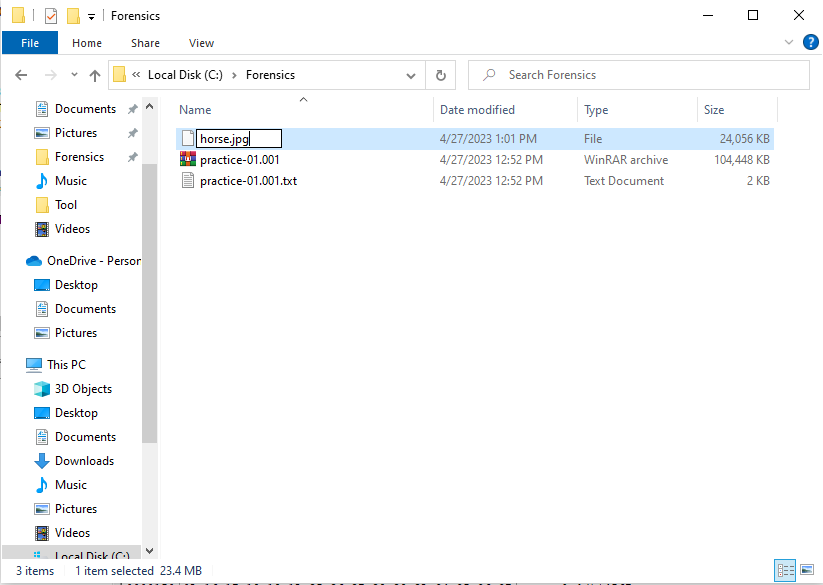


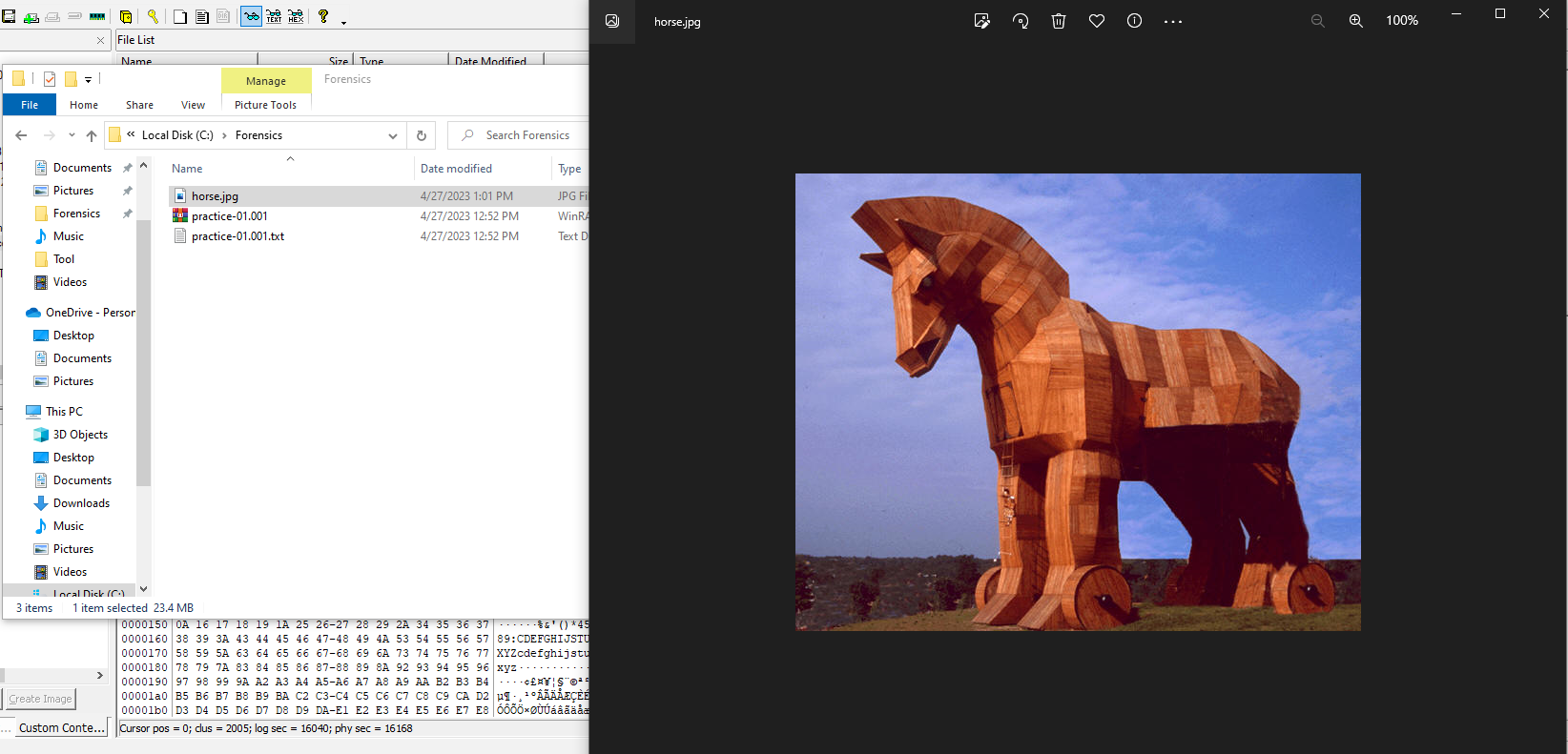
**View deleted file(s) in unallocated space**



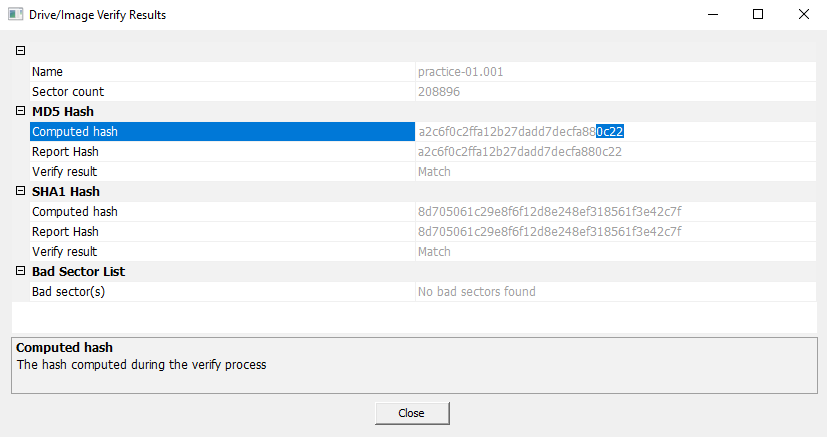
**Recover file and rename**





**Last 4 characters: 0c22**



**Prof**

