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

**Objective:**

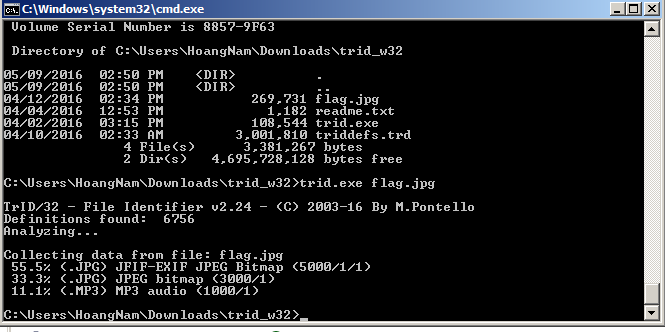
HexView to view header about JPEG to understanding FILE HEADER

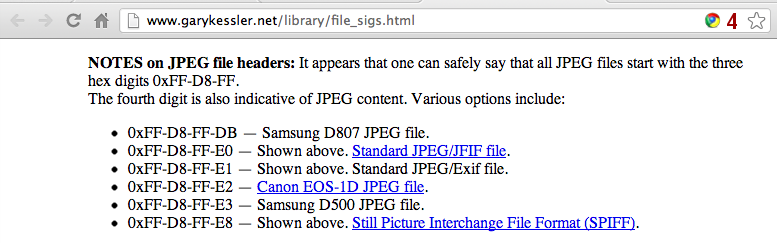
**What You Need for This Lab**

* + A Windows machine, real or virtual
  + A identify tool, such as Trid
  + A Hex editor, such as HxD

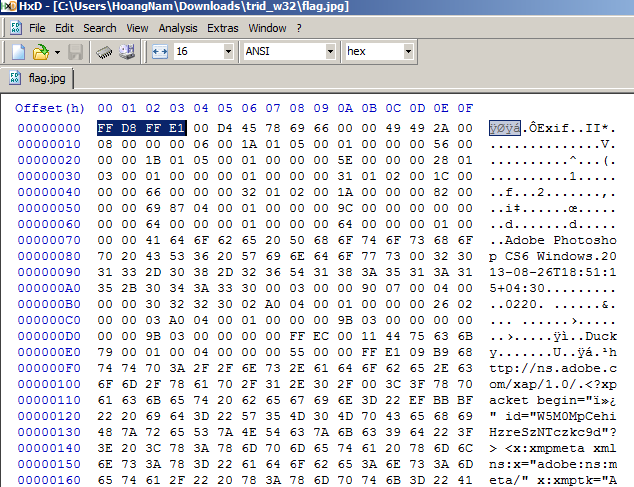
**Download the Image file:** [**http://localhost/flag.jpg**](http://localhost/flag.jpg)

**Opening the Trid and HxD for identify and view header image file:**

****



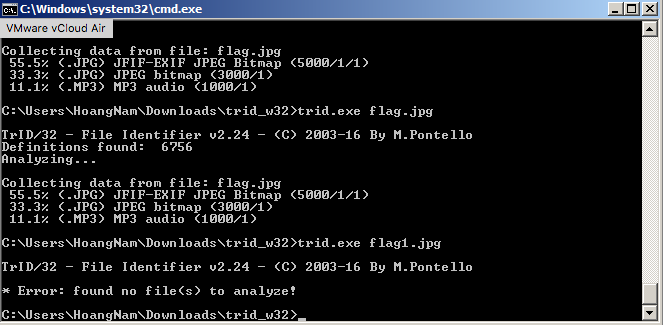
**View header JPEG by HexView**

****

**Mofify FF-D8-FF-E1 to FF-D8-FF-E2 you can not see the picture.**

****

**Trid can not identify the flag file**

****

1. **Rebuilding an Image Header**

**What You Need for This Project**

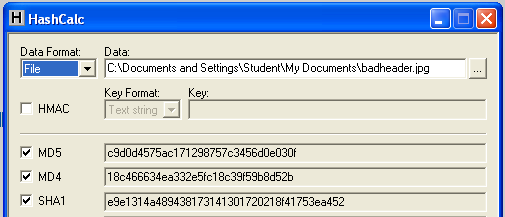
* A Windows machine, real or virtual
* A hex editor, such as HxD

**Downloading the Image File**

Right-click the link below and save the file on your desktop:

[badheader.jpg](https://samsclass.info/121/proj/badheader.jpg)

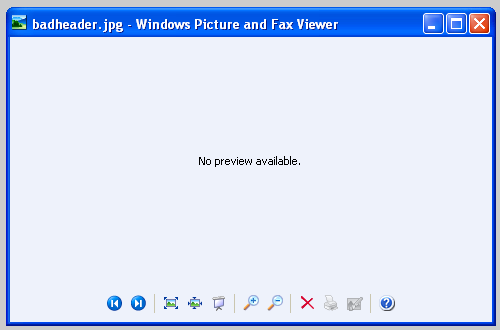
Using HashCalc or some similar program, verify the MD5 hash of your downloaded file. The correct hash value is shown below:



**Opening the Image File**

On your desktop, double-click the **badheader.jpg** file.

You see an error message, as shown below:

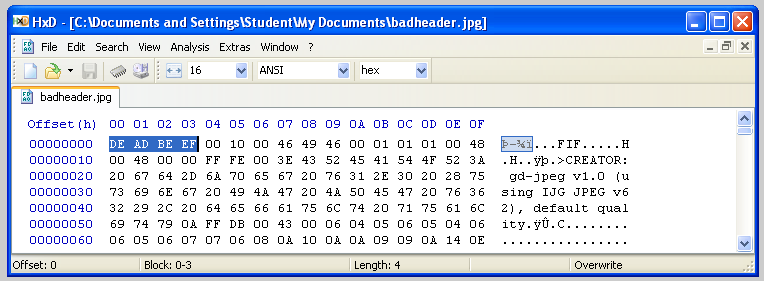


**Viewing the File in a Hex Editor**

Open the **badheader.jpg** file in HxD.

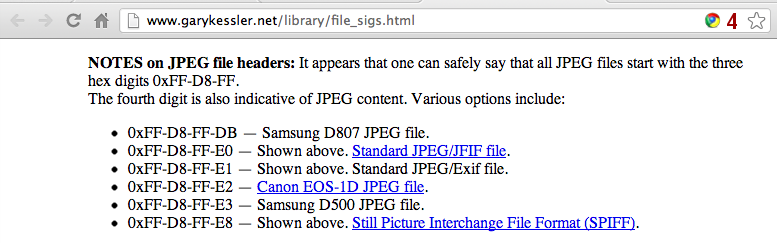
*If you don't have HxD, download it from:* [*http://mh-nexus.de/en/hxd/*](http://mh-nexus.de/en/hxd/)

The header looks wrong--it starts with DE AD BE EF, as shown below:



So to fix it, you need to find out what a good JPG header looks like.

You can use online resources like this:



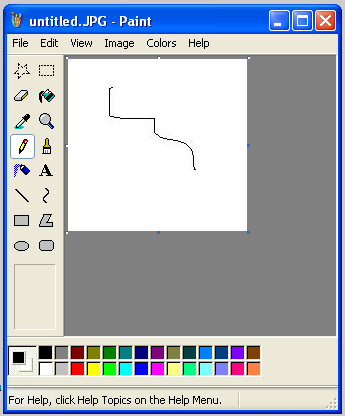
From <http://www.garykessler.net/library/file_sigs.html>

But a simpler way is to just examine a good JPG.

**Examining a Good JPG File**

Open Paint.

Draw or scribble something, as shown below:

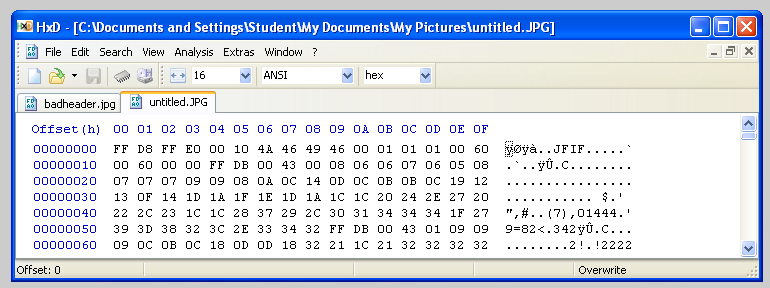


Click **File**, **Save**.

Save the file as a JPG.

Open the file you just created in HxD.

The first few bytes are different--not DE AD BE EF, but FF D8 FF E0 as shown below:

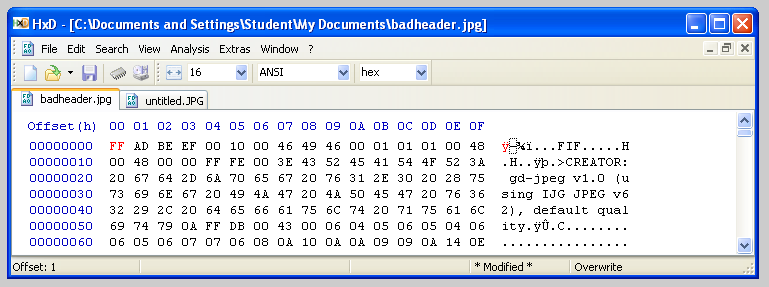


**Repairing the Header**

In HxD, with "badheader.jpg" open in the left pane, click on the first byte, which now is DE.

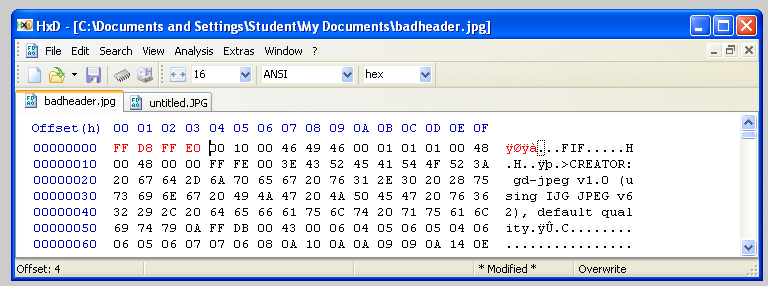
Type over it with **FF**

The changed letters turn red, as shown below:



Continue in the same manner to fix the first four bytes of the file in HxD.

Your file should now look like the image below:



**Saving the File**

In HxD, click **File**, **Save**.

**Viewing the Image**

On your desktop, double-click the **badheader.jpg** file.

The image should open correctly now, showing a wooden window frame with a cat looking through it.

**Saving a Screen Image**

Make sure the **image of a cat** is visible.

Press the PrintScrn key in the upper-right portion of the keyboard. That will copy the whole desktop to the clipboard.

**YOU MUST SUBMIT A FULL-SCREEN IMAGE TO GET FULL CREDIT!**

Open Paint and paste in the image.

Save the image with the filename "**Your Name** ". Use your real name, not the literal text "Your Name".