## CIT 430/530 - Forensic Activity 1.6 – File Carving with dd

In this activity you will carve an image out of raw data using the dd program. DD is a “command-line utility for Unix and Unix-like operating systems, the primary purpose of which is to convert and copy files”. Although dd was not originally designed for computer forensics, it has become a defacto tool many investigators are familiar with.

**References:**

“A Comprehensive Beginner’s Guide to Linux as a Digital Forensic Platform” - Barry J. Grundy. [<https://linuxleo.com/>]

## Setup

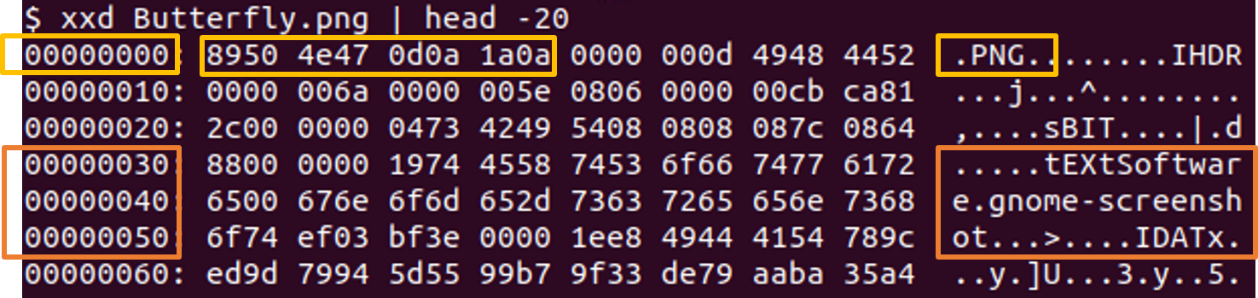
Change to the Downloads directory and open the .raw file with the hex dump tool xxd.

**# xxd image\_carv\_2017.raw | less**

It’s really just a file full of random characters. Somewhere inside there is a standard JPEG image. Let’s go through the steps we need to take to recover the picture file using dd and other Linux tools.

## File Carving

In the example below, xxd was used to view a PNG image. Notice in the output the PNG file signature (highlighted in yellow), starts at hexadecimal offset row 0x00, file signature 8950 4E47 0D0A 1A0A. The second highlighted portion (in orange) provides information about the image itself. While this is not a file signature, it does show the readable text string “Software gnome-screenshot” begins at hexadecimal offset row 0x30 and ends at 0x50.



A JPEG has a standard file signature starting with **ffd8** in hexadecimal. The string ‘ffd8’ is common and will most likely be found by xxd in multiple places. The key is to also look for additional hexadecimal strings confirming this is a JPEG image.

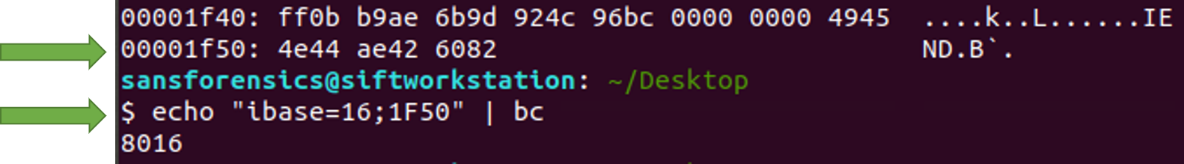
In this case, find a **ffd8** string that is followed by the hex characters **ffe00 0104a** **4a46 4946**, the file signature of JFIF format for sending images over the Internet.

**# xxd image\_carve\_2017.raw | grep ffd8**

1. **What offset row contains the JPEG and JFIF signatures?** 
   1. **36ac0**

To carve out the image, we’ll need every byte, including file headers and footers. In the next step you’ll use a simple calculator to convert the offset row hexadecimal found in question number 1 to decimal.

* *Note: ‘Hex\_Row’ is a placeholder and should be replaced with the value returned in question #1*.
* If the hexdecimal number contains letters, capitalize them and do not include any leading zero in the command



**# echo “ibase=16;Hex\_Row” | bc**

1. **What decimal number was returned?** 
   1. **223936**

The resulting number is the decimal representation of the row where the JPEG image starts in xxd. To find the end of the JPEG file, we’ll use the starting row number in decimal from question 2, plus six bytes because the JPEG file signature starts 6 bytes within the row itself and the standard file trailer signature of **ffd9**.

* **Add 6** to the Decimal\_Start value to account for the files physical starting position within the raw image file. If this is not done, the image viewer won’t be able to tell the type of image type it’s trying to open.

**# xxd -s Decimal\_Start image\_carv\_2017.raw | grep ffd9**

1. **What row (i.e. offset) hex value was returned indicating the files end?**
   1. **5d3d0**
2. **What value is this in decimal?** 
   1. **381904**

The full size of the image can now be calculated by subtracting the decimal value representing the beginning of the file from the end of file decimal value.

1. **What is the size of the image to be carved?** 
   1. **381894-223942 = 157952**

If the above was done correctly, the jpeg can now be carved from the raw data using the program dd and the following options:

* **skip** = number of bytes skipped to reach the start of the image. *Use the decimal value from question #2*.
* **bs** = number of bytes per block
* **count** = number of blocks carved out of the raw data. *Use the decimal value from question #5*.

**# dd if=image\_carve\_2017.raw of=carved.jpg bs=1 skip=Q2\_value count=Q5\_value**

If no errors are reported, you’ll see an output of total bytes copied and the amount of time to complete the carve.

1. **Screenshot this information and insert it below**. If errors are returned, go back and double-check your calculations.
   1. A screenshot of a dog

      Description automatically generated with medium confidence

View your work with the command below.

**# eog carved.jpg**

## Submission

After successfully carving the image from the data, upload a completed version of this document to Canvas.