**File Carving:**

Carving an image from the disk “image\_carve.raw”

Knowing the type of file. One method of carving is using header/footer information

JPEG files start with ffd8 and ends with ffd9

**Tools used:**

xxd hexadecimal viewer

grep Finding strings

bc Linux calculator utility

dd to copy the selected segment to a file

**Step 1: Find the start of jpeg**

xxd image\_carve | grep ffd8 Find the block address which contains string ffd8

Use bc find decimal value for block address echo “ibase=16;0x5DER” | bc

**Step 2: Find the end of jpeg**

xxd image\_carve | grep ffd9 Find the block address which contains string ffd8

Use bc find decimal value for block address echo “ibase=16;0x5DER” | bc

**Step 3: Calculate the size of the file in bytes**

**Step 4: Copy the block containing the bytes of jpeg file**

dd if=image\_carve.raw of=carv.jpg skip=21156 bs=1 count=6610

count total number of bytes

bs block size (Set to 1)

skip starting byte address