CS 50 Walkthrough 5

Problem Set 5: Forensics

Keito Uchiyama

Problem Set 5: Forensics

- Topics:
  - File I/O
  - Data structures, hexadecimal, and pointers
- Programs:
  - whodunit
  - resize
  - recover

Bitmaps

- Each pixel's color is represented as levels of Blue, Green, and Red.

  [00-ff] [00-ff] [00-ff]

- A bitmap is a series of consecutive pixels described after each other.
- Also has "metadata" in first 54 bytes consisting of two headers.

Smiley ☺

```
xxd -c 24 -g 3 -s 54 smiley.bmp
```

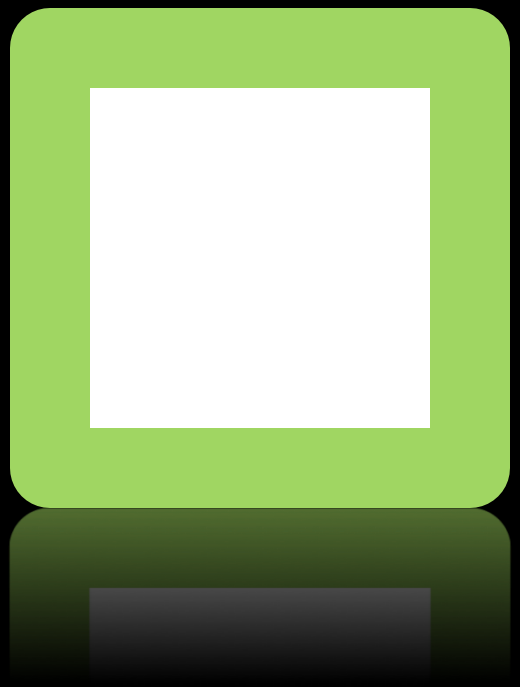
Smiley ☺

```
ffffff ffffff 0000ff 0000ff 0000ff 0000ff ffffff ffffff
ffffff 0000ff ffffff ffffff ffffff ffffff 0000ff ffffff
0000ff ffffff 0000ff ffffff ffffff 0000ff ffffff 0000ff
0000ff ffffff ffffff ffffff ffffff ffffff ffffff 0000ff
0000ff ffffff 0000ff ffffff ffffff 0000ff ffffff 0000ff
0000ff ffffff ffffff 0000ff 0000ff ffffff ffffff 0000ff
ffffff 0000ff ffffff ffffff ffffff ffffff 0000ff ffffff
ffffff ffffff 0000ff 0000ff 0000ff 0000ff ffffff ffffff
```

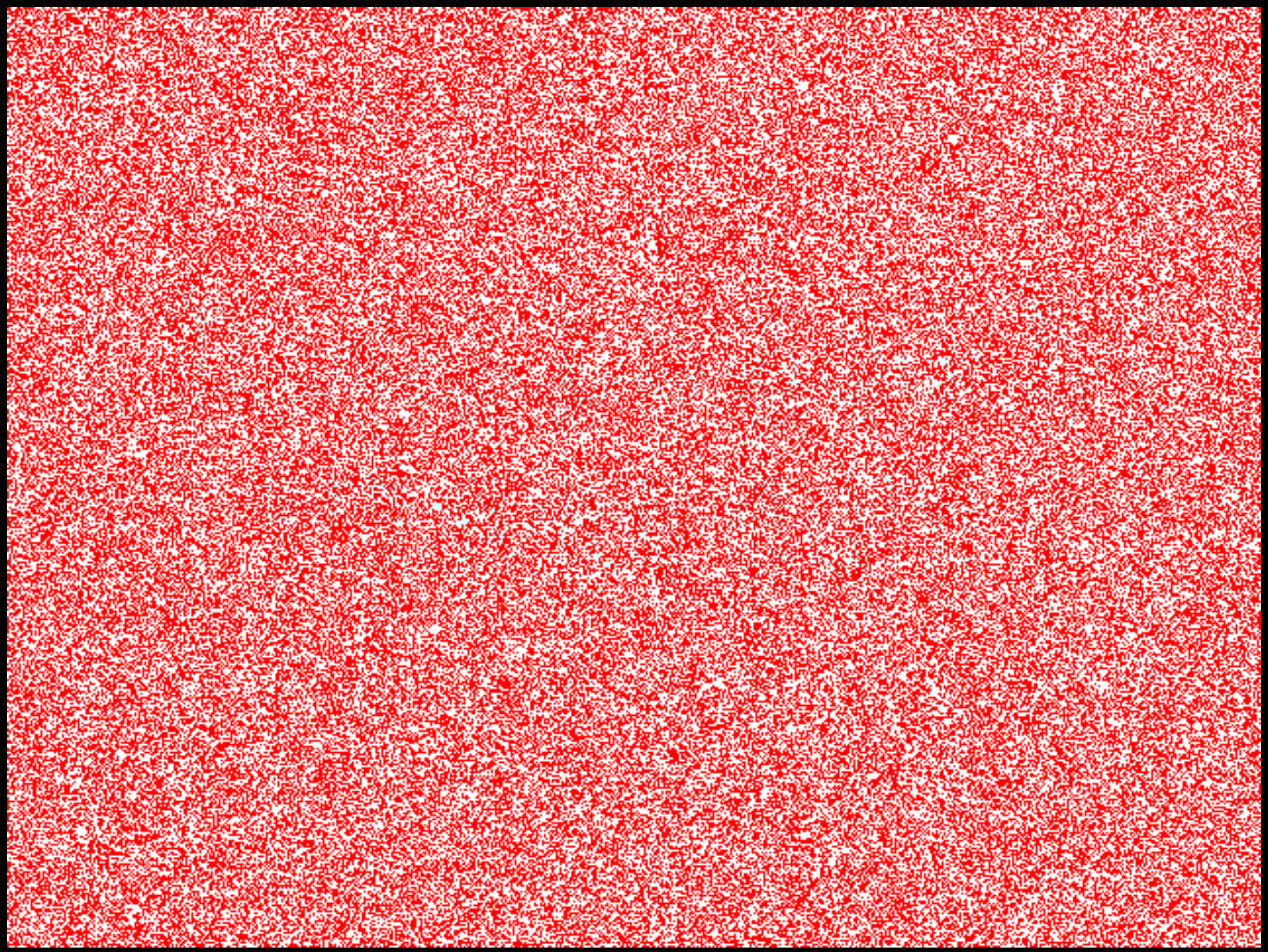
Bitmap Headers

offset	type	name	
0	WORD	bfType	BITMAPFILEHEADER
2	DWORD	bfSize	
6	WORD	bfReserved1	
8	WORD	bfReserved2	
10	DWORD	bOffBits	
14	DWORD	biSize	BITMAPINFOHEADER
18	LONG	biWidth	
22	LONG	biHeight	
26	WORD	biPlanes	
28	WORD	biBitCount	
30	DWORD	biCompression	
34	DWORD	biSizeImage	
38	LONG	biXPelsPerMeter	
42	LONG	biYPelsPerMeter	
46	DWORD	biClrUsed	
50	DWORD	biClrImportant	
54	BYTE	rgbtBlue	RGBTRIPLE
55	BYTE	rgbtGreen	
56	BYTE	rgbtRed	
57	BYTE	rgbtBlue	RGBTRIPLE
58	BYTE	rgbtGreen	
59	BYTE	rgbtRed	
...			
243	BYTE	rgbtBlue	RGBTRIPLE
244	BYTE	rgbtGreen	
245	BYTE	rgbtRed	

Bitmap padding



Whodunit?



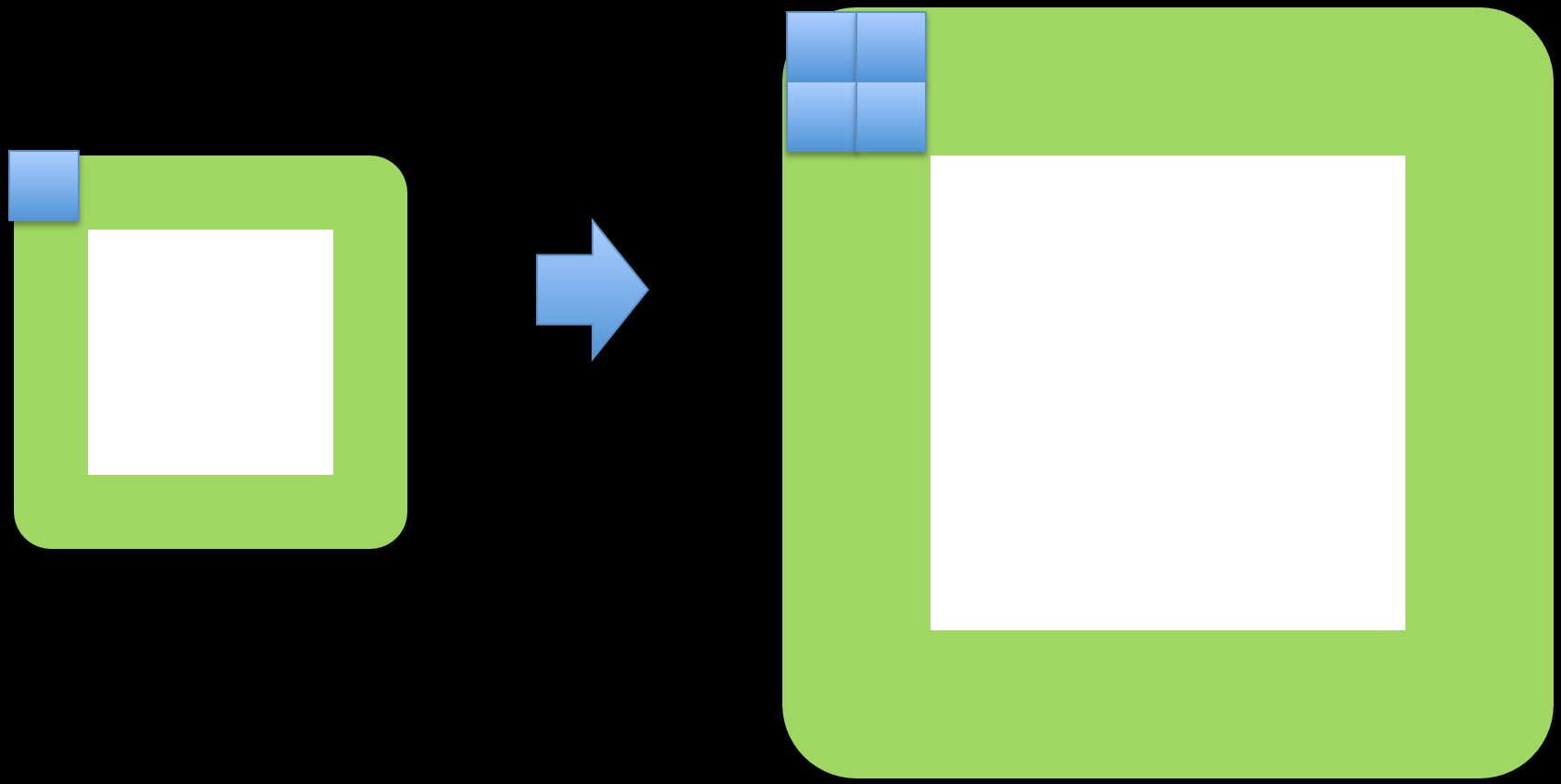
Resize

- Two steps:
  - Make necessary changes to the metadata
  - Write out the new pixels
- We can use the same copy.c framework!

Resize - Metadata

offset	type	name	
0	WORD	bfType	BITMAPFILEHEADER
2	DWORD	bfSize	
6	WORD	bfReserved1	
8	WORD	bfReserved2	
10	DWORD	bOffBits	
14	DWORD	biSize	BITMAPINFOHEADER
18	LONG	biWidth	
22	LONG	biHeight	
26	WORD	biPlanes	
28	WORD	biBitCount	
30	DWORD	biCompression	
34	DWORD	biSizeImage	
38	LONG	biXPelsPerMeter	
42	LONG	biYPelsPerMeter	
46	DWORD	biClrUsed	
50	DWORD	biClrImportant	
54	BYTE	rgbtBlue	

Resize - Pixels



```
resize 4 small.bmp large.bmp
```

Image recovery!

```
0000000: ff d8 ff e0 00 10 4a 46  ......JF
0000008: 49 46 00 01 01 01 00 60  IF.....`
0000010: 00 60 00 00 ff e1 1d da  .`......
0000018: 45 78 69 66 00 00 49 49  Exif..II
0000020: 2a 00 08 00 00 00 0a 00  *.......
0000028: 0f 01 02 00 12 00 00 00  ........
0000030: 86 00 00 00 10 01 02 00  ........
0000038: 0b 00 00 00 98 00 00 00  ........
0000040: 12 01 03 00 01 00 00 00  ........
0000048: 00 00 00 00 1a 01 05 00  ........
```

Image recovery - Steps

- Steps:

  Go through each block in the disk image and:

  1. If we find a JPEG signature, start writing the bytes out to another file
  2. If we find a new JPEG signature, close that old file and go back to 2
  3. If we find the End Of File, close the file and kthxbai

CS 50 Walkthrough 5

Problem Set 5: Forensics

Keito Uchiyama