F20FO Lab 3

File Structure & Data Recovery

Chandrashekhar R (cr2007)

Contents

Lab 3.1: Number Systems 2
Complete the following conversion table: 2
Complete the following table: 2
Lab 3.2: File Structure 2
File Signatures 2
What is the correct file extension for this file? 2
What does it contain? 2
JPEG Signature 3
Can you identify which one was shot with a Canon camera? (Hint: use a hex editor) 3
Which of these images uses EXIF? 3
Lab 3.3: File Carving I 3
Can you see the PNG header in the file anywhere? 3
Note the location of the header and footer, so that you can easily find them again. 3
Lab 3.4: File Carving II 3
In your document write a short description about what you retrieved. 3

Lab 3.1: Number Systems

Complete the following conversion table:

Current State	Binary (unsigned)	Hexadecimal
203_{10}	11001011	**CB_{16}**
10999_{10}	**10101011110111_{2}**	2AF7
54	**110110_{2}**	**36_{16}**

Complete the following table:

Colour	Hex Code RGB	Decimal Code RGB
Colour1	AB 65 2F	124 0 63
Red	**FF 00 00**	**255 0 0**
Green	**00 FF 00**	**0 255 0**
Blue	**00 00 FF**	**0 0 255**
White	**FF FF FF**	**255 255 255**

Lab 3.2: File Structure

File Signatures

What is the correct file extension for this file?

The correct file extension is `.jpeg`.

What does it contain?

It contains a picture of a man wearing a white shirt and a striped tie.

JPEG Signature

Can you identify which one was shot with a Canon camera? (Hint: use a hex editor)

'*Img3.jpg*' was shot using a Canon camera.

When you open up the JPG image file using Frhed, the application marker displayed in the image contents was '**`FF E1`**', indicating that the image uses a **Ex**changeable **I**mage **F**ormat (EXIF).

Upon further inspection of the file, using the hex editor Frhed, we were able to see the extra information showed within the file, including the fact that the image was shot with a Canon camera.

Which of these images uses EXIF?

- Img3.JPG

Lab 3.3: File Carving I

Can you see the PNG header in the file anywhere?

Yes, the PNG header is visible in Offset `386 (0x182)`

Note the location of the header and footer, so that you can easily find them again.

- **Header:** Offset `386 (0x182)` to `389 (0x185)` (`.PNG`)
- **Footer:** Offset `3634 (0xe32)` to `3637 (0xe35)` (`IEND`)

Lab 3.4: File Carving II

In your document write a short description about what you retrieved.

The retrieved data reveals a total of eight distinct items.

Among these items are a single video file encoded in AVI format, accompanied by a collection of four images in JPG format, although one image showed signs of potential corruption.

Additionally, our examination uncovered a ZIP archive containing a solitary text file, alongside a pair of enigmatic empty files whose formats remain unidentified.

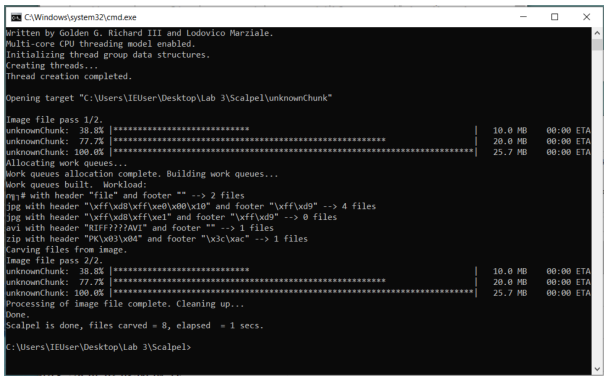

Figure 1: Scalpel command execution
