Recupero

By team QED

James Whitcroft

Samuel Launt

Carus Cookman

Table of Contents

Illustration Index

Revisions

Date	Changes	Who
3/14/17	Base Creation	Samuel Launt

Introduction

Recupero is a file recovery program designed for the ext2 file system. The purpose of this project is to learn more about the ext2 file system and Linux in general.

Recupero works by reading the inode bitmap and looking to see if the inode is free, then looking to see what data blocks it points to. It then looks at the data bit map to see if those blocks are free and not over written. If all all blocks aren’t overwritten then the file will be recovered.

There will be other functionality as well, it will be able to do the following:

- Recover data
- Print super block information
- recover from a corrupt super block
- print an inode
- print the inode/data bit map from a group block
- print meta data about the file system
- print the group descriptor

Project Layout

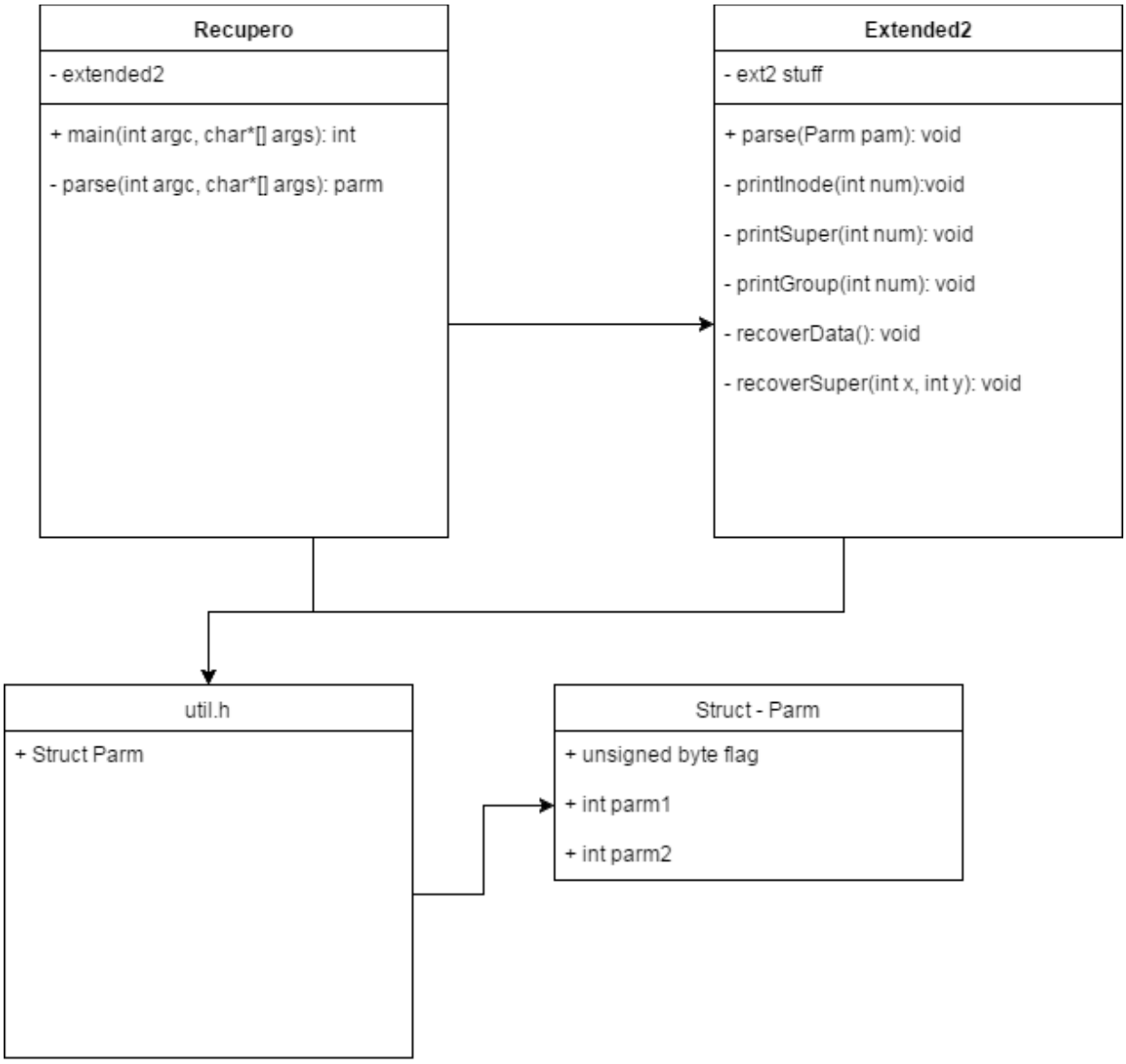

Illustration 1: UML

From this you can see that the main class only takes in the command line input and parses the command. It will use a struct called parm to pass the commands to the extended2 object. This object will then interpret the commands and perform the right action.

Program Flow

There is a potential issue with this program using to much RAM. To prevent this there should ever be more than a full group block in memory.

No matter the command passed the extented2 object there should always be a check to make sure the target is an EXT2 file system and if it is run a method for meta-data collection. This

includes, but not limited to how many group blocks there are, block size, number of blocks, number and location of super blocks.

For the prints of the super blocks and group descriptors is pretty much the same. Offset to the proper location read in the target and print it out to screen.

For printing of the meta data, just print the data collected from the meta-data method.

For Recovering data the flow should go something like this:

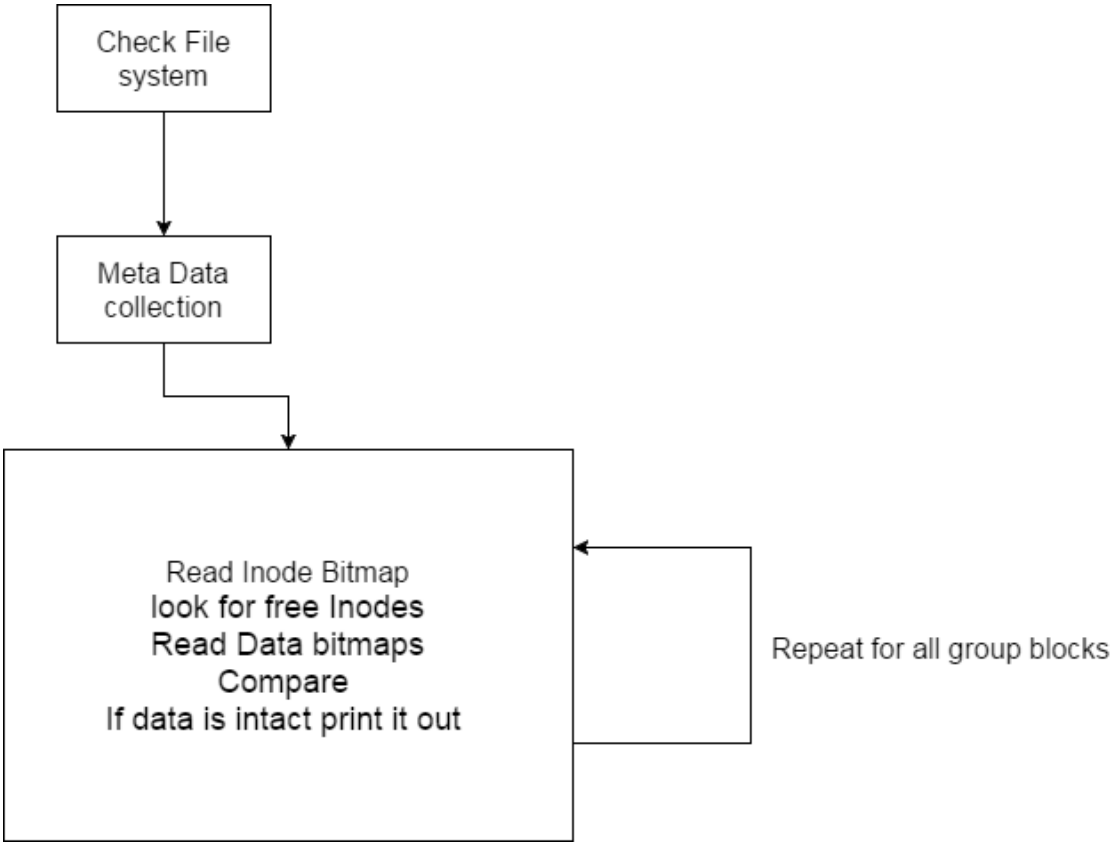

Illustration 2: data recovery flow

Lastly for the recovery of the super blocks. This is just overwriting the first super block with the second. So an offset read, offset write.

Recupero Interface

There should be 2 ways of interacting with recupero, from a single command line command or from an interactive interface. For example the user should be able to use the command “$ sudo recupero print inode 6 /dev/sda2”. Or from an interactive interface like “sudo recupero /dev/sda2” then be promted with “<recupero> #”. From there be able to perform repeated commands.

The commands are as follows:

- print inode <number>
- print superblock <number>
- print meta
- print bitmap <inode/data> <number>
- recover data
- recover superblock <num> <num>

Sprints

This project will be conducted in 2 main sprints. The first is for core functionality. This is recovering data. Part 2 will be all the other functions. Part 3 is for stretch goals as of time of writing there aren't any, but if they come up they will be done here.

Testing

For testing there are a few test cases for recovering data:

1. Small file (few bytes)
2. medium file (couple hundred megs)
3. large file (couple gigs)

These tests will be performed on:

1. mounted file 512mb
2. mounted second hhd 20gb