Digital Forensics Project

We look at two file systems – NTFS (windows) and Ext (linux). For our purpose, ext2, ext3, ext4 are same (for the time being).

The first main section is to define the objective of the project.

The second section describes the structure of the file systems

# Objective

Files system can be corrupted accidently or by human action. We want to recover the file system as much as possible. This means mainly two things:

1. The meta data should be recovered
2. The individual files AND the directories are recovered (the “lost” files and directories may be due to drive crashes or the action of deleting the file/directories).
3. Analyze what percentage of the disk has been recovered.

We will develop tools to achieve these objectives and use heuristics and other techniques to recover files.

# Boot sector

### Description

The first block of all hard drives, no matter what type of file system (NTFS or EXT etc), contains the boot sector.

### Types of Corruption

What can happen if boot sector is corrupted? Partition data can be lost.

1. Number of partitions on the hard drive?
2. Type of partition?
3. Size of partition?

### Recovery

How to recover this partition data?

# EXT FILE SYSTEM

The file system is divided into block groups. Each block group mainly consists of the following blocks:

* Super block
* Group Descriptors
* Data Block bitmap
* Inode bitmap
* Inode table
* Data blocks

## Super Block

### Description

### Type of Corruption

### Recovery

## Group Descriptors

### Description

### Type of Corruption

### Recovery

## Data Block Bitmap

### Description

### Type of Corruption

### Recovery

## Inode Bitmap

### Description

### Type of Corruption

### Recovery

## Inode Table

### Description

### Type of Corruption

### Recovery

## Data Blocks

### Description

### Type of Corruption

### Recovery

# NTFS FILE SYSTEM

# FILE TYPE EXTENSIONS

This section describes the various file types, eg jpeg, pdf etc. Each file type has a certain format. The sections below will describe the format of each file type. This will help in recovering the files.

Note: I have added the following extensions so far. Feel free to volunteer and add other well known extensions.

### Format of jpg extension

### Format of png extension

### Format of wav extension

### Format of mpg extension

### Format of flv extension

### Format of pdf extension

### Format of tiff extension

### Format of doc extension