

The Analysis and Classification of Deleted-file Overwrite Characteristics in Common Usage Scenarios (ACDOCINCUS)

by

**Lloyd Carothers, Dan Driscoll, Robert Erbes,
James Kearney**



Overview

- **Introduction to Project**
- **Development of Model**
- **System Simulation**
- **Analysis of Simulation Results**



Introduction

The Whys and Whats



Introduction

- **Motivating questions:**
 - **How long does it take for a deleted file to get overwritten?**
 - **What's the probability of (relatively) easy recovery?**
 - **What can we expect from recovery efforts?**
 - **Is there a difference in Time to Loss between different file systems?**
 - **If so, What?**



Model Development

How How How How How How



Model Development

- **Derived from empirical evidence**
- **Used to simulate file I/O on production systems**
- **Constraints:**
 - **access patterns**
 - **static file size**
 - **file system**

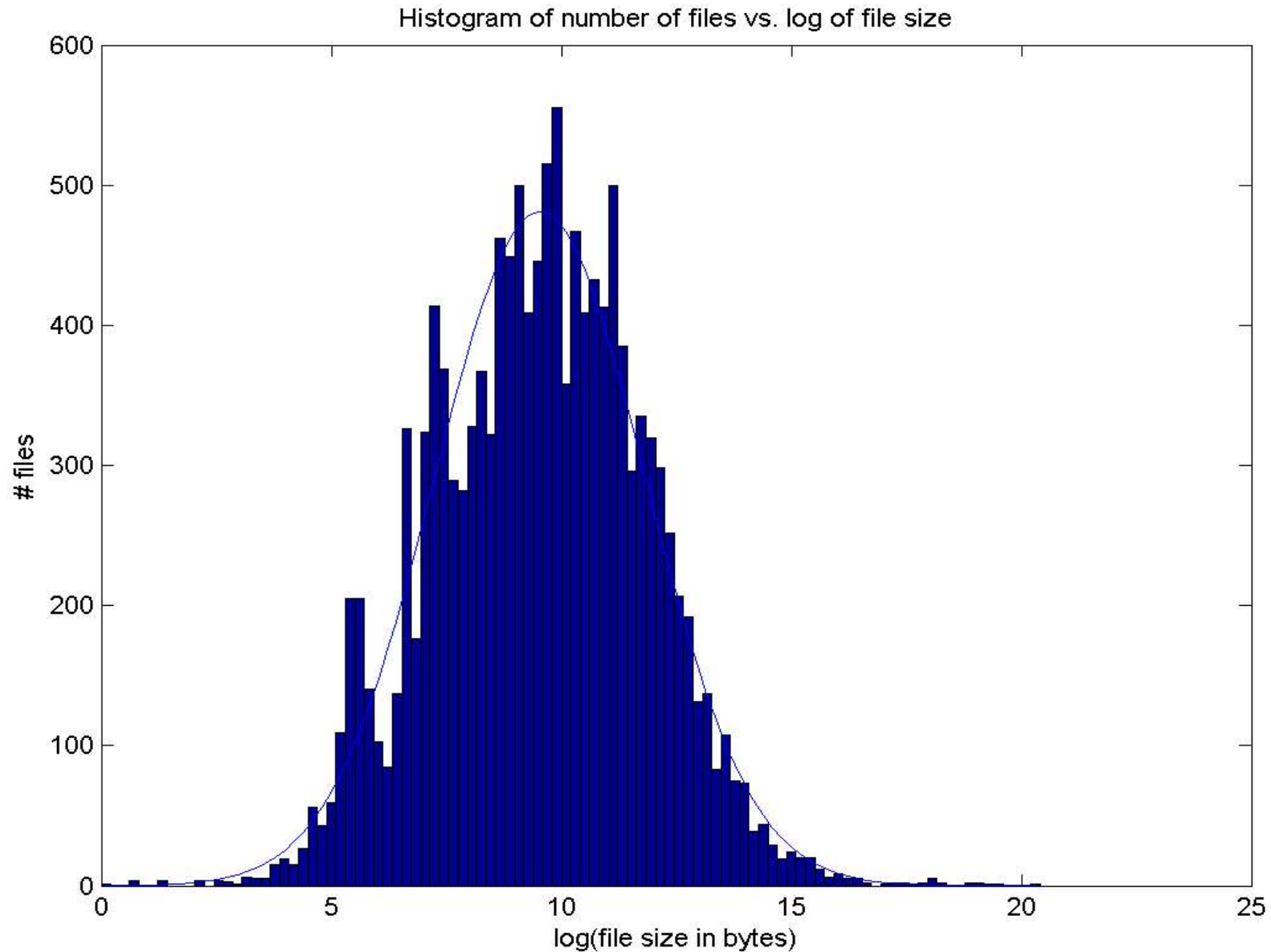
Model Development

Log-normal (mean, std. dev) of File Size > 0

	μ	σ	P_z
Windows	9.267	2.265	0.002
Linux	8.873	2.548	0.012
Linux Fileserver	7.575	1.911	0.028
All	8.534	2.203	0.014

P_z = % of zero length files

Model Development



Model Development

- **Relevant Assumptions:**
 - **File creations and deletions of any given filesize are balanced**
 - **Rate of file creation/deletion = probability of existence for that filesize**
 - **Overall freespace utilization (in file creation) is based on a proportion of drive space available**

System Simulation

Create and Destroy

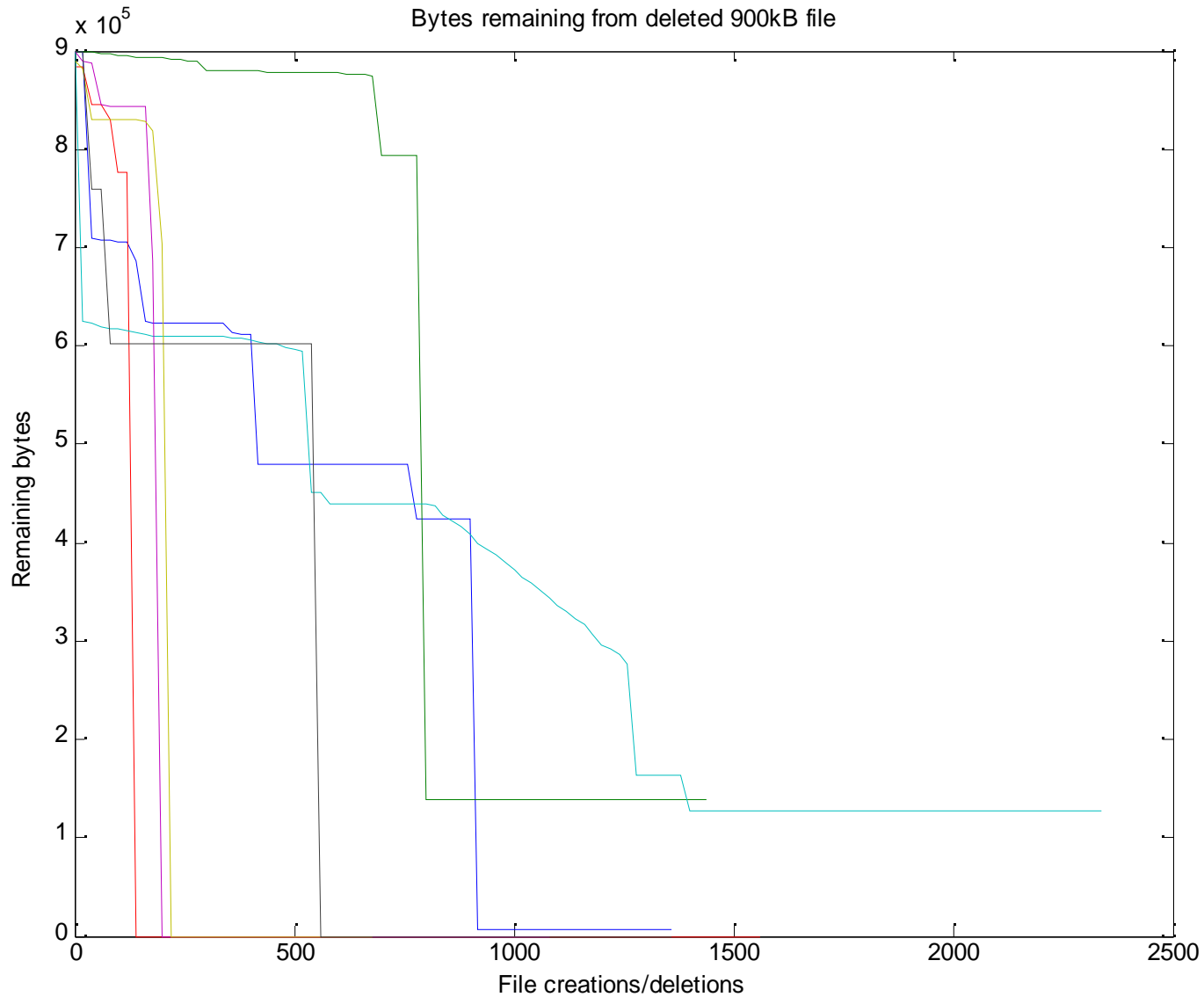
System Simulation

- **Process:**
 - Prime empty drive to achieve valid representation
 - Random creation/deletion of files according to model
 - Ongoing generation of analysis output of file system at fixed intervals

Analysis of Simulation Results

Damnit Holmes!

Analysis of Simulation Results



Conclusion

Waste of time?

Conclude THIS!

Conclusion (ext2)

- **Nearly all data loss is due to big files (yeah)**
- **Nearly all files show immediate partial data loss**
- **Complete file loss very early on for some cases**
 - **< 200 file accesses (create/delete)**
- **Some cases preserved data for a very long time**

Conclusion (ext2 vs. FAT32)

- **FAT32**
 - 46k c/d before extinction
 - 1/3 of cases had initial partial file loss
- **ext2**
 - 2k c/d before extinction

Questions

?