

Change-Link: A Digital Forensic Tool for Visualizing Changes to Directory Trees

Change-Link: A Digital Forensic Tool for Visualizing Changes to Directory Trees

Timothy R. Leschke
Cyber Defense Lab
University of Maryland, Baltimore County
Baltimore, MD 21250
tleschk1@umbc.edu

Alan T. Sherman
Cyber Defense Lab
University of Maryland, Baltimore County
Baltimore, MD 21250
sherman@umbc.edu

ABSTRACT

We present Change-Link, a customizable data exploration tool which empowers the user to see visual representations of directories that have changed over time within a computer operating system. It supports the Microsoft Volume Shadow Copy Service (VSS). Change-Link displays change information in a split-screen interface comprising an overview of directory change for the entire dataset and a detail view of change for individual directories. Input to Change-Link is an evidence hard drive containing an active file system and previous versions of the directory structure that were archived by the VSS. This approach to browsing change within a directory structure helps a digital forensic examiner understand how a particular volume was used to support criminal activity. Because data that has changed are often the most important, identifying directories that have changed over time directs attention towards data of higher importance. By examining the most important data, digital forensic examiners are better able to keep pace with the data explosion that is making current digital forensic examinations unmanageable. Our contributions include the development of a *segmented bar and whisker* glyph for representing change over time for individual directories; an approach for aggregating VSS data in digital forensic examinations; and a data visualization tool for exploring digital forensic data.

Categories and Subject Descriptors

H.I [Models and Principles]: User/Machine Systems—*Human Information Processing* ; H.5 [Information Interfaces and Presentation]: User

© 2012 Association for Computing Machinery. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of the United States government. As such, the United States Government retains a non-exclusive, royalty-free right to publish or reproduce this article or to allow others to do so, for Government purposes only.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior written permission or a fee.
ViSec '12 October 15 2012, Seattle, WA, USA
Copyright 2012 ACM 978-1-4503-1413-8/12/10...\$15.00.

Interfaces—*Screen Design and User-Centered Design*

Keywords

Coordinated and multiple views, linked view, change over time, overview+detail, digital forensics, data visualization.

1. INTRODUCTION

Digital forensics involves extracting and analyzing data from digital artifacts in support of law enforcement investigations. The term “digital forensic examination” is used to describe the rapid growth in recent years of the amount of data that is subject to a digital forensic examination. This data explosion is fueled by the increased capacity and decreased cost of computer hard drives, and the proliferation of smart phones, GPS receivers, and other portable devices that have growing digital storage capacities. As a result, persons engaged in criminal activity are being associated with larger amounts of digital evidence. The amount of data that digital forensic examiners must analyze become unmanageable. We design, implement, and demonstrate a new data visualization tool to help address this data explosion.

One way to keep pace with the data explosion is to increase the bandwidth by which digital forensic examiners perceive forensic data. Because more information can be obtained through vision than through all other senses combined [1], obtaining information through data visualization presents the greatest bandwidth for human perception. The need for an increased perceptual bandwidth is one of the primary motivations for applying data visualization techniques to digital forensics. Other motivations include knowledge discovery, increased productivity, and better comprehension [1].

By understanding how digital evidence has changed over time, digital forensic examiners are better able to understand what happened. A notable computer process that records data that have changed over time is the Microsoft Volume Shadow Copy Service (VSS), which is found in Windows Vista and Windows 7. A representation of data that are created by this service are known as shadow volumes.

According to Microsoft, there can be as many as 512 shadow volumes for a given volume [13]. Current digital forensic tools support the assessing of individual shadow volumes, and some provide an understanding of what changed between two selected shadow volumes. None of the known tools support an understanding of change over multiple shadow volumes, and certainly none scale well enough to convey change according to as many as 512 shadow volumes.



Timothy R. Leschke, M.S.
Doctoral Student
tleschk1@umbc.edu



Alan T. Sherman, Ph.D.
Associate Professor
sherman@umbc.edu

Motivation

- Visualizing Change
- Digital Forensics
 - Data Explosion
 - Shadow Volume Data



Benefits of Visualizing Change

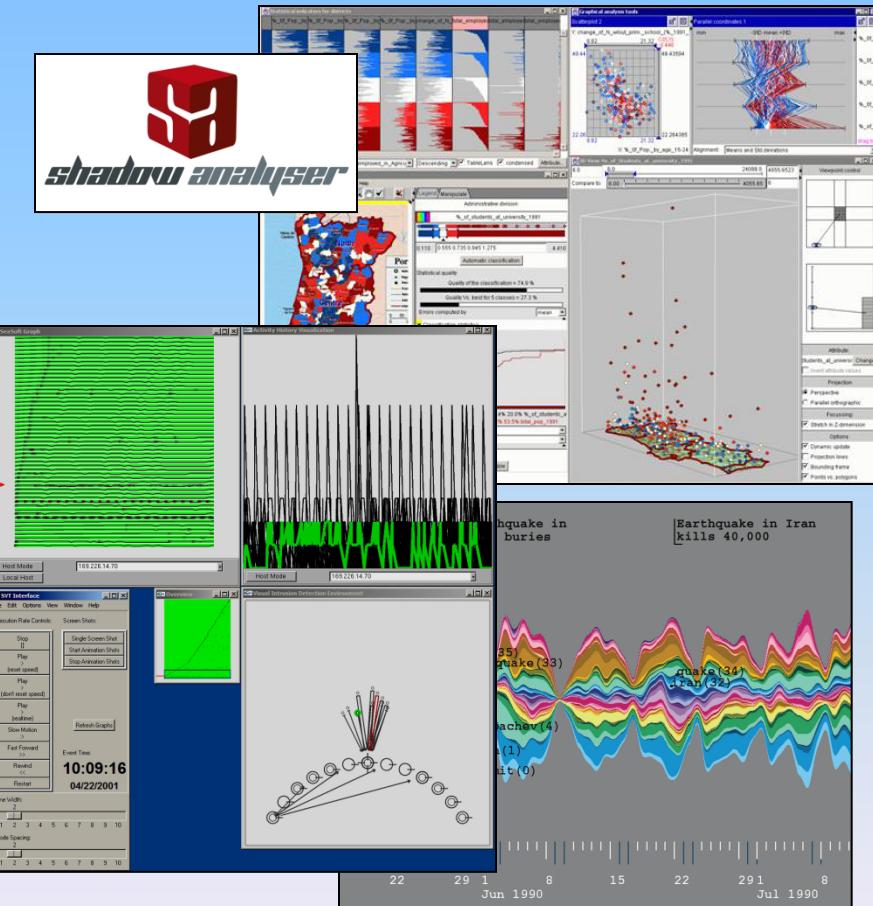
- “...direct their efforts toward more important data.”



- “...digital forensic examiners are better able to understand what happened.”

Related Work

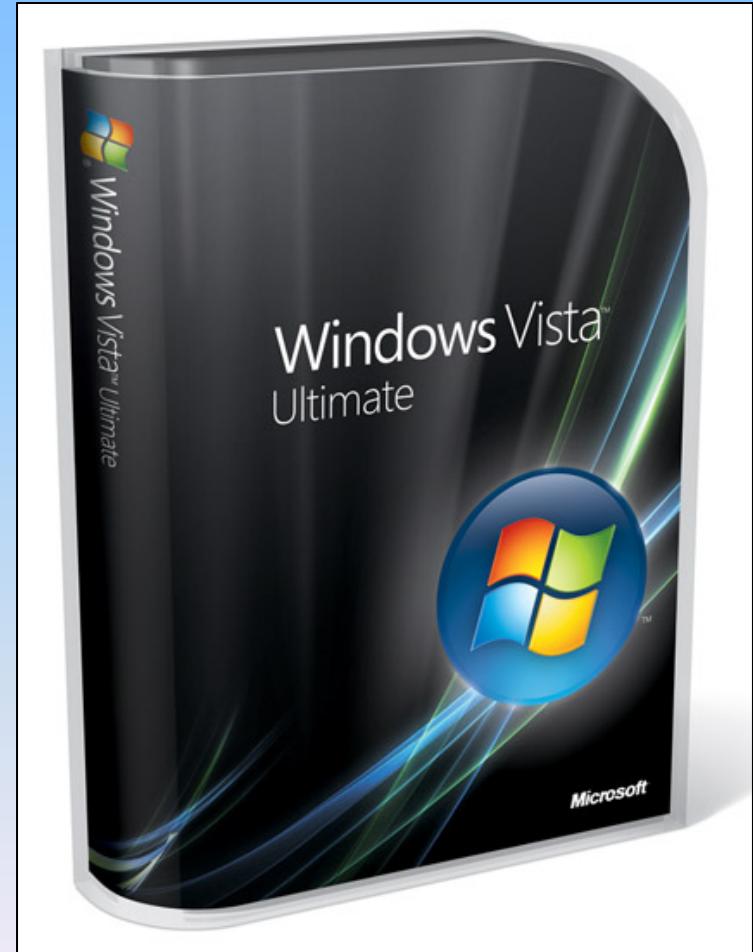
- Shadow Volume Tools
- Coordinated and Multiple Views
- Visual Analytics
- Linked Views
- Overview+Detail
- TreeJuxtaposer & Mizbee
- Visualization of Change
 - Few address *coming into* and *going out of* existence.



<http://www.prlog.org/10766636-shadow-analyser-computer-forensics-tool-for-digital-forensic-investigators.jpg>, State of the Art: Coordinated & Multiple Views in Exploratory Visualization by Jonathan C. Roberts, Hierarchical Linked Views by Erbacher and Frincke, Themeriver: Visualizing thematic changes in large document collections, by Havre, Hetzler, Whitney and Nowell.

Shadow Volume Data

- Volume Shadow Copy Service
 - Windows Vista, Windows 7, and others
- When data is archived
 - Backup utility
 - Prior to installation
 - Restore point
- Why data is archived
 - Rollback data to restore stability and recover lost data.

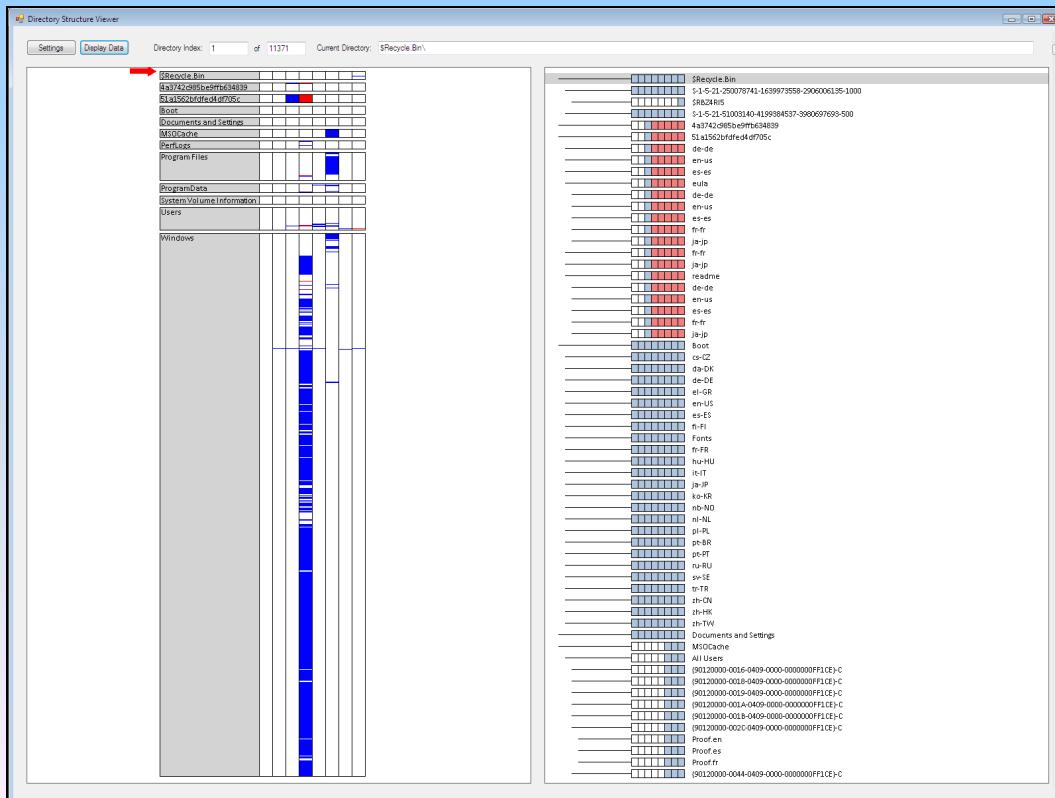
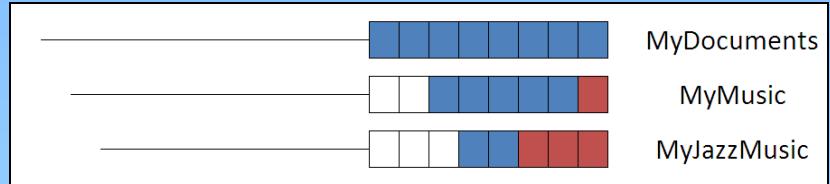
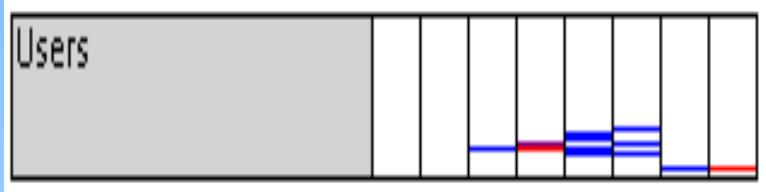


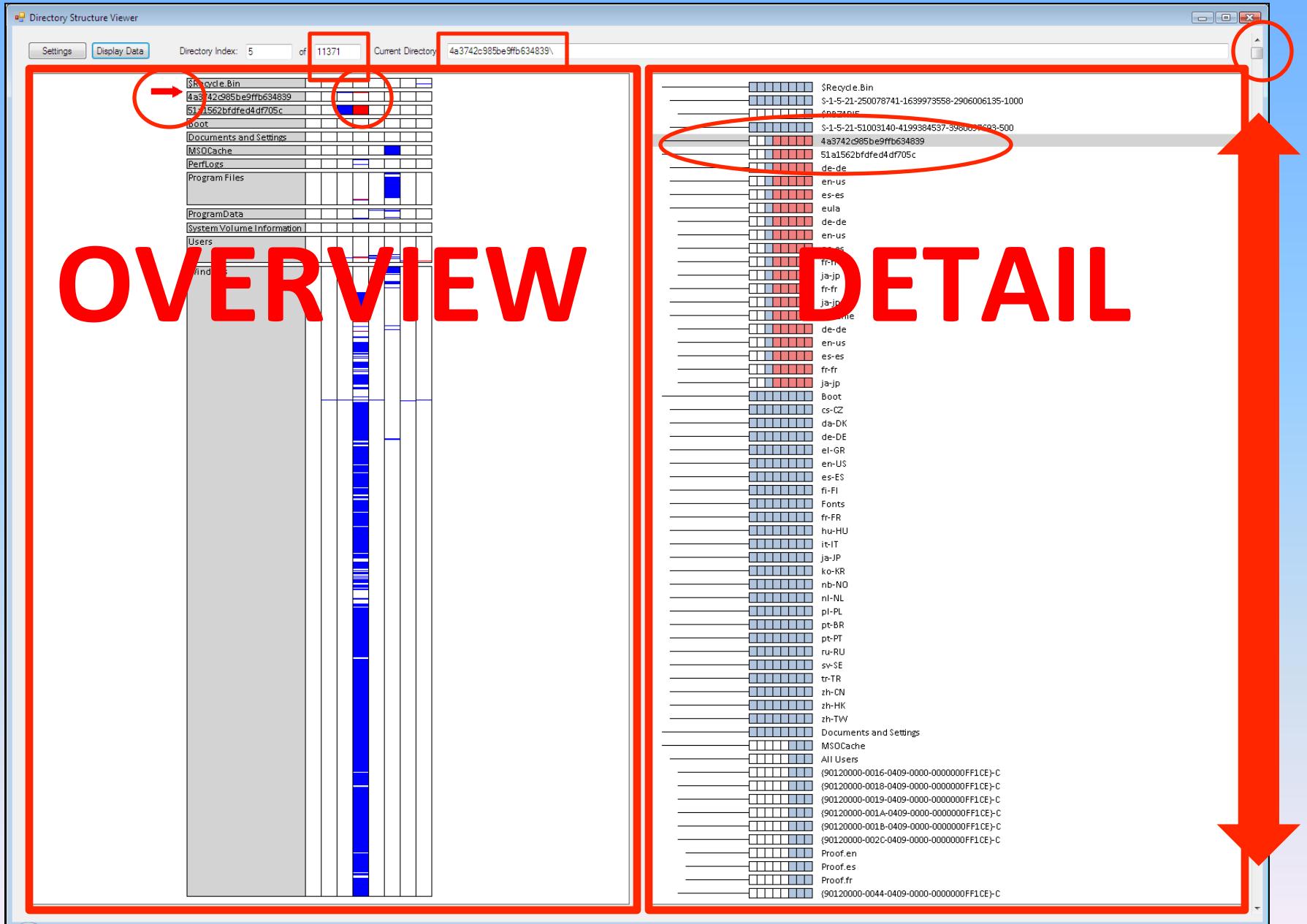
Test Data

- Eight shadow volumes
 - After installing Vista
 - After activating Vista
 - During installation of SP1
 - After installing SP1
 - After installing Office
 - After activation of Office
 - After creating directories
 - After deleting directories
- 11,000 directories x 8 shadow volumes = 88,000 data points.
- 700,000 directories x 8 ≈ 5 million data points!

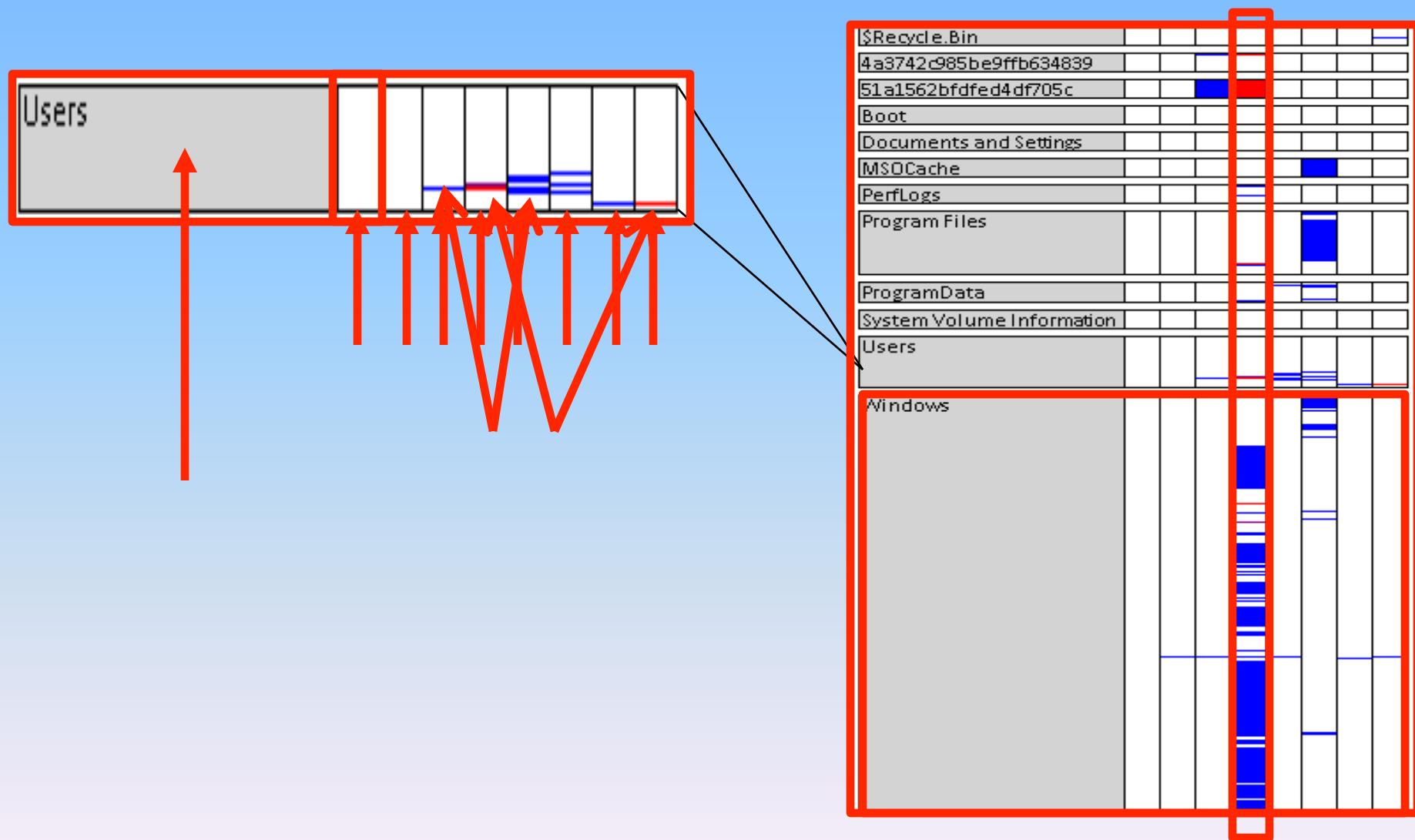


Design and Implementation

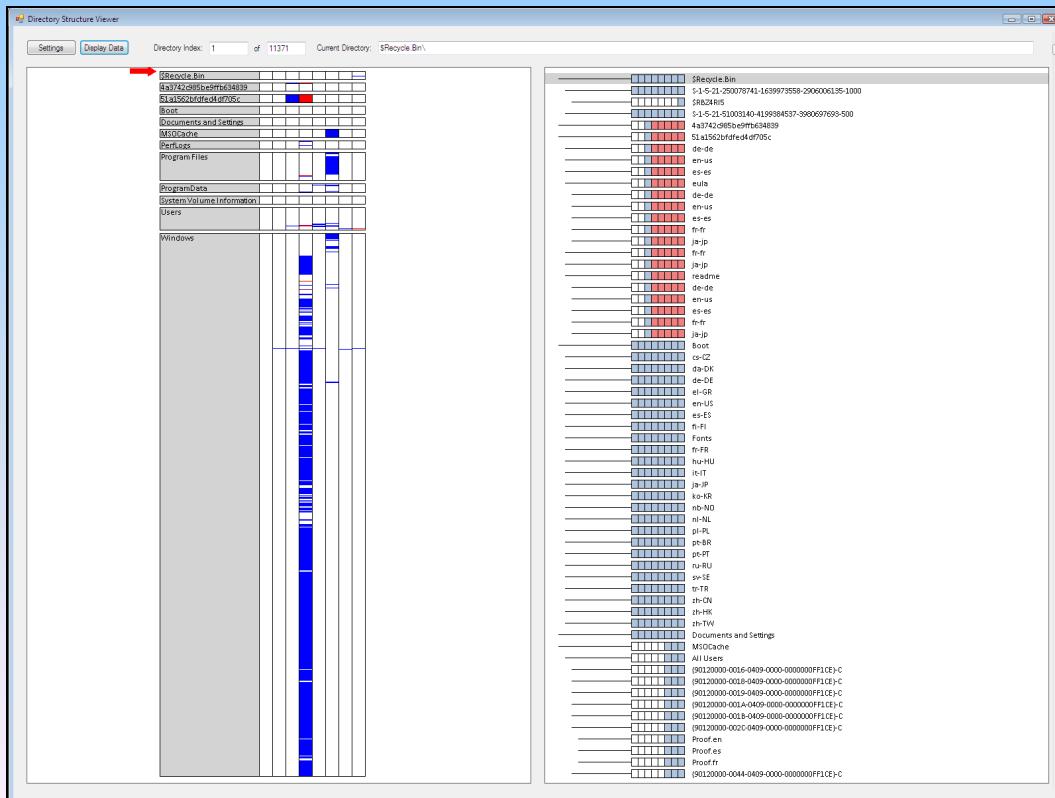
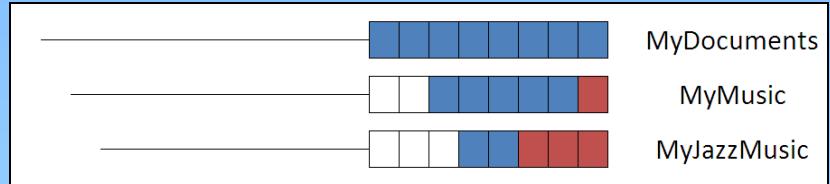
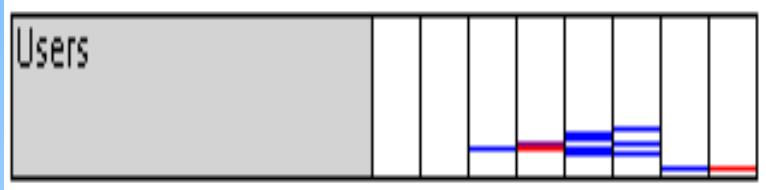




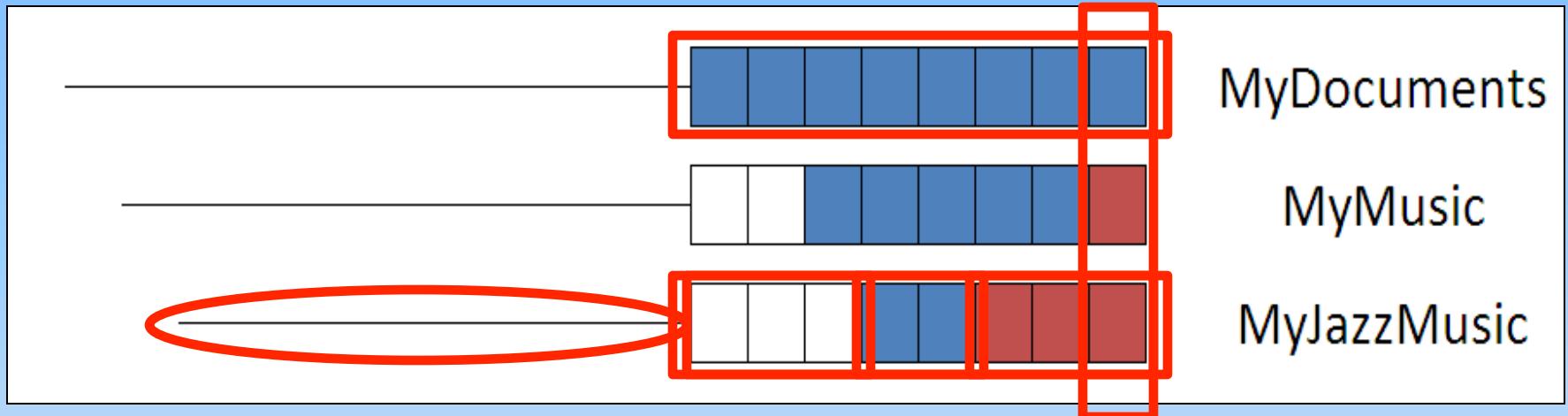
Overview Window

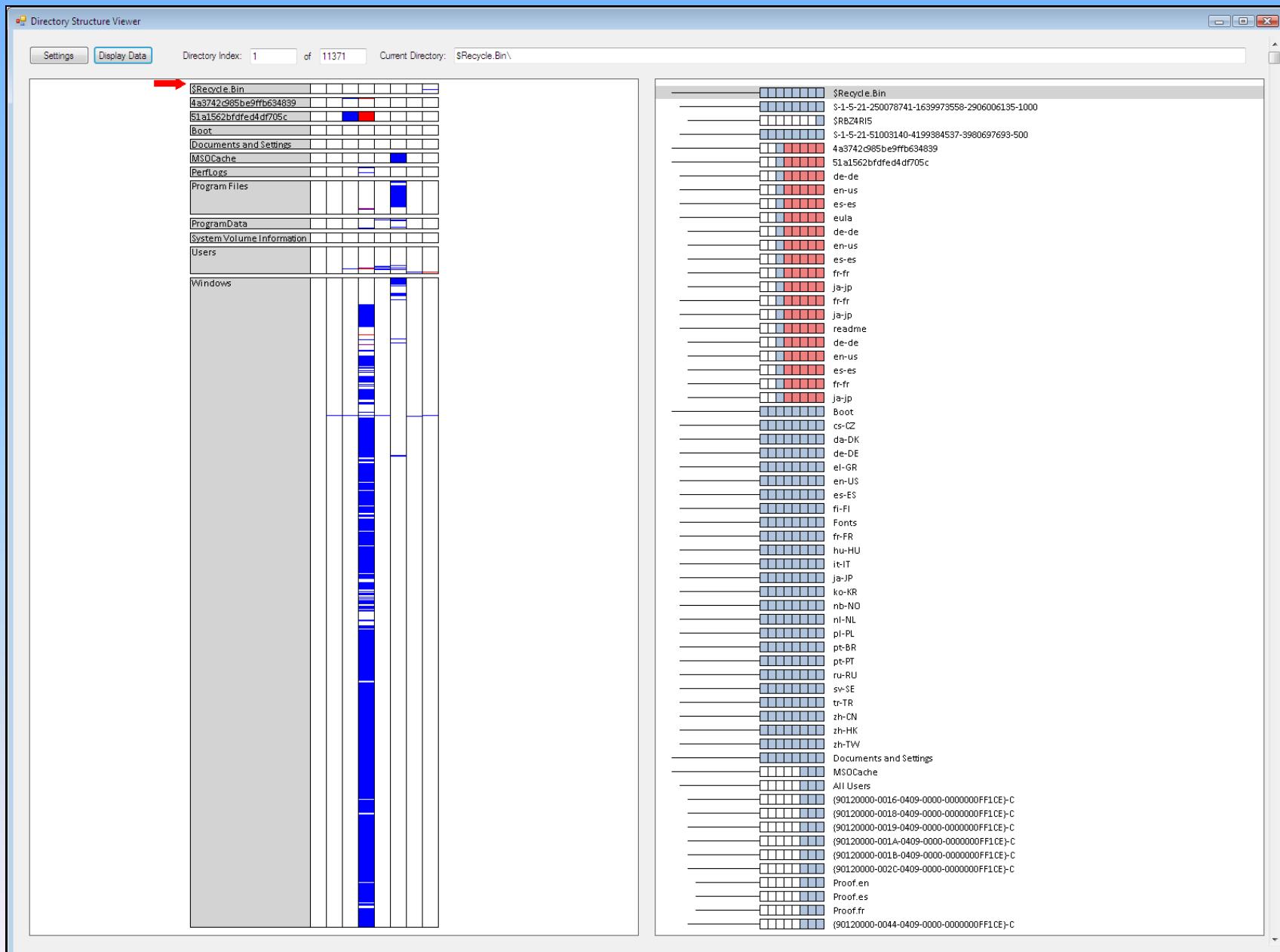


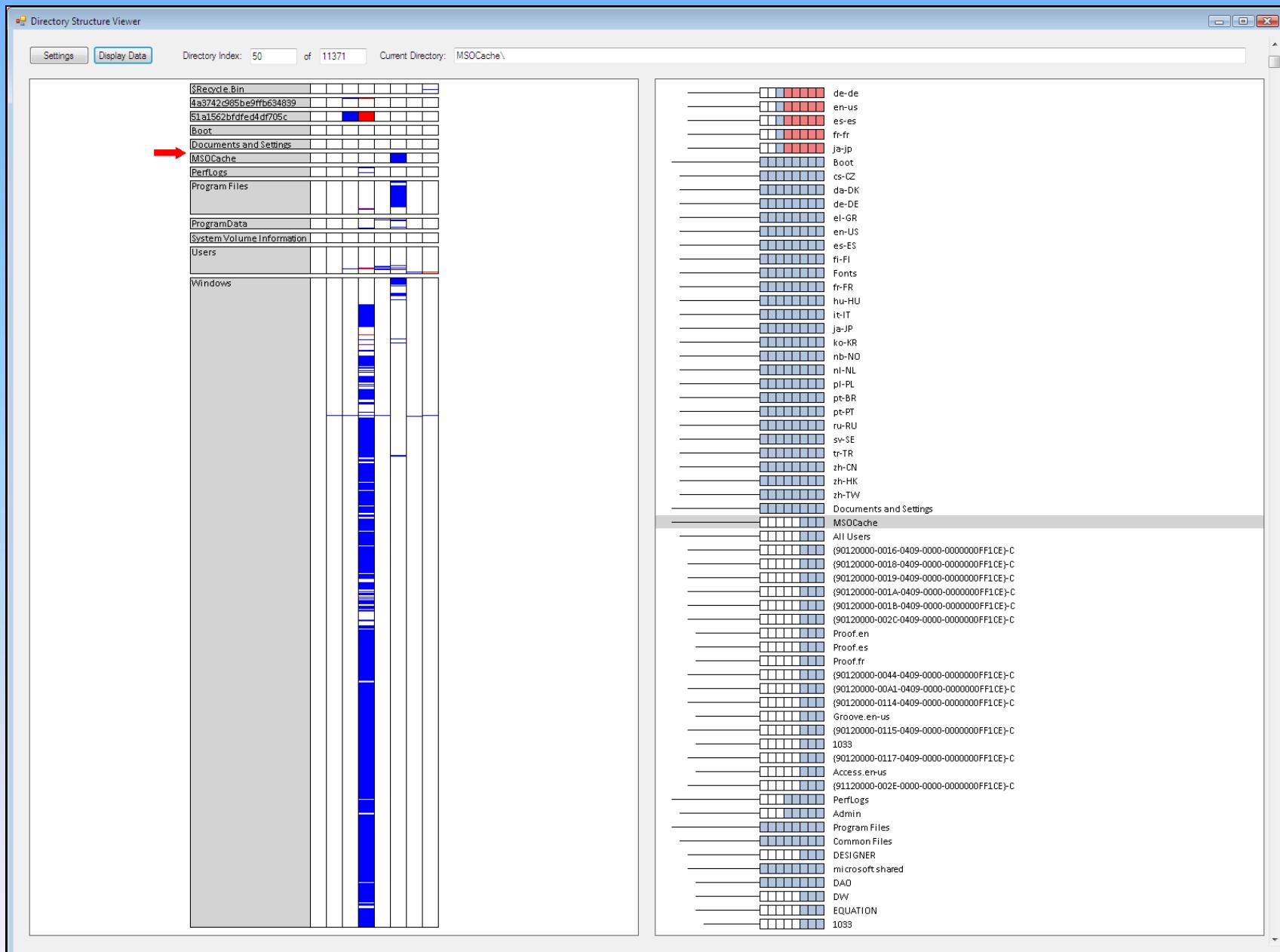
Design and Implementation

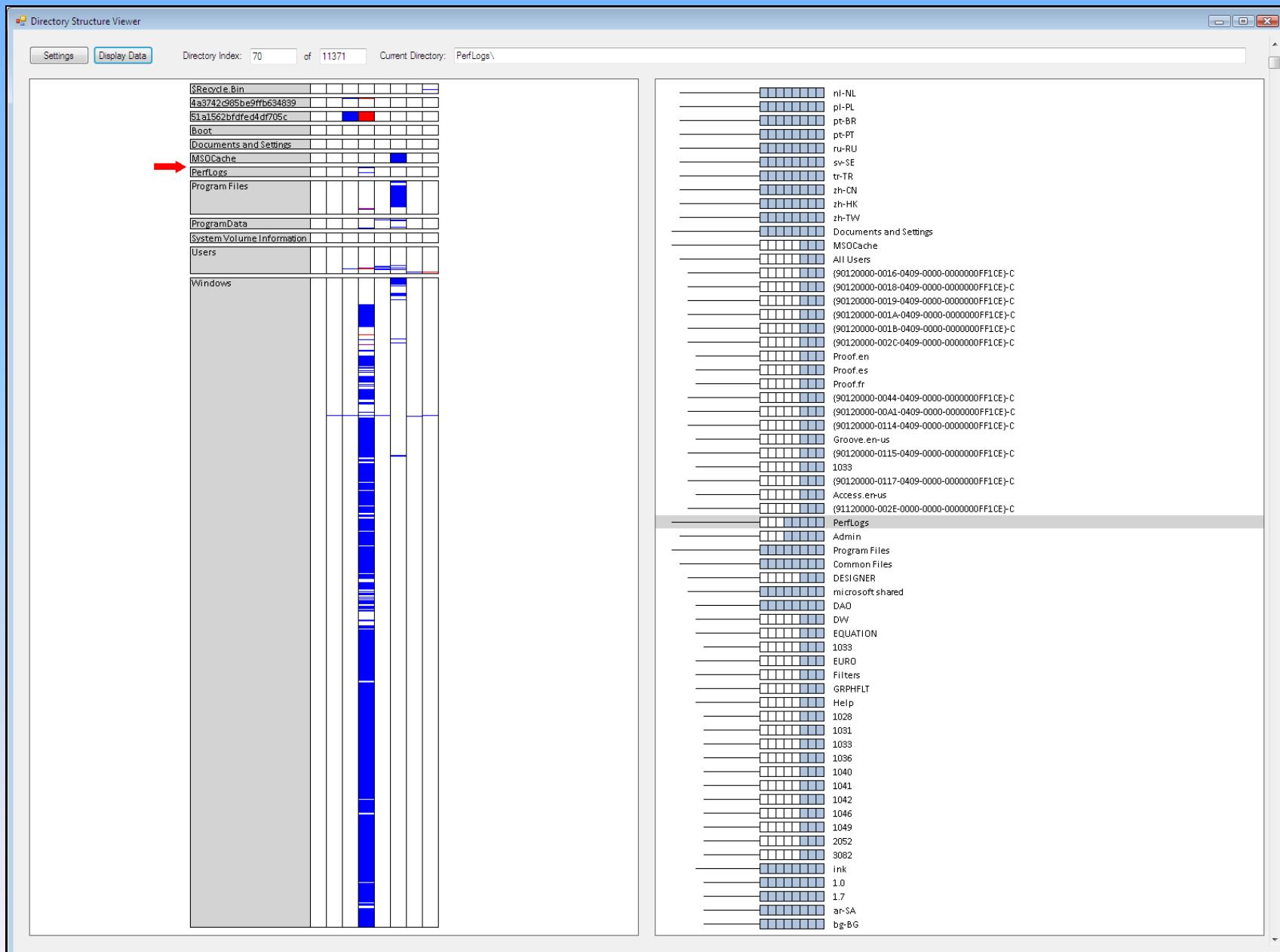


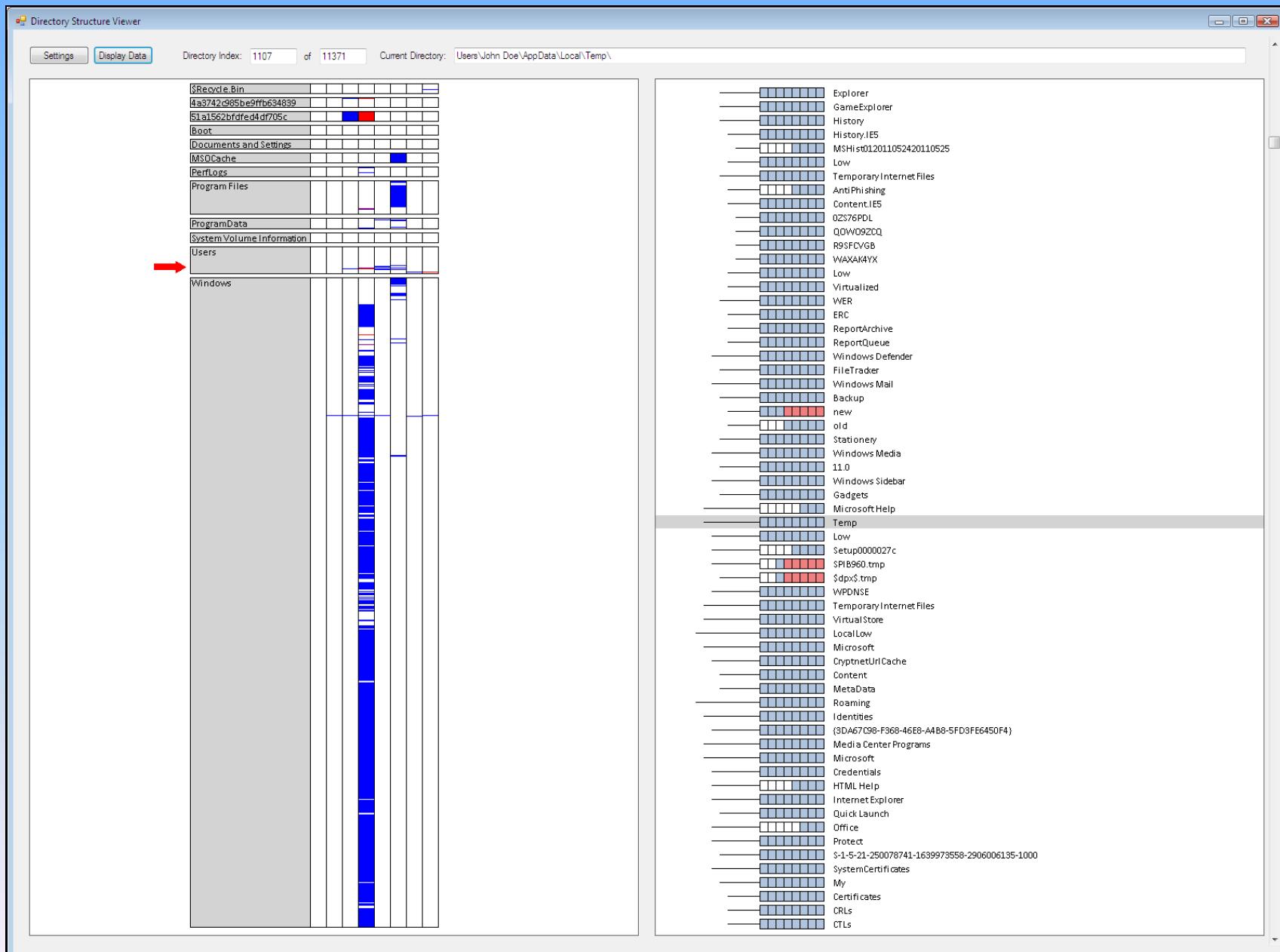
Segmented Box and Whisker

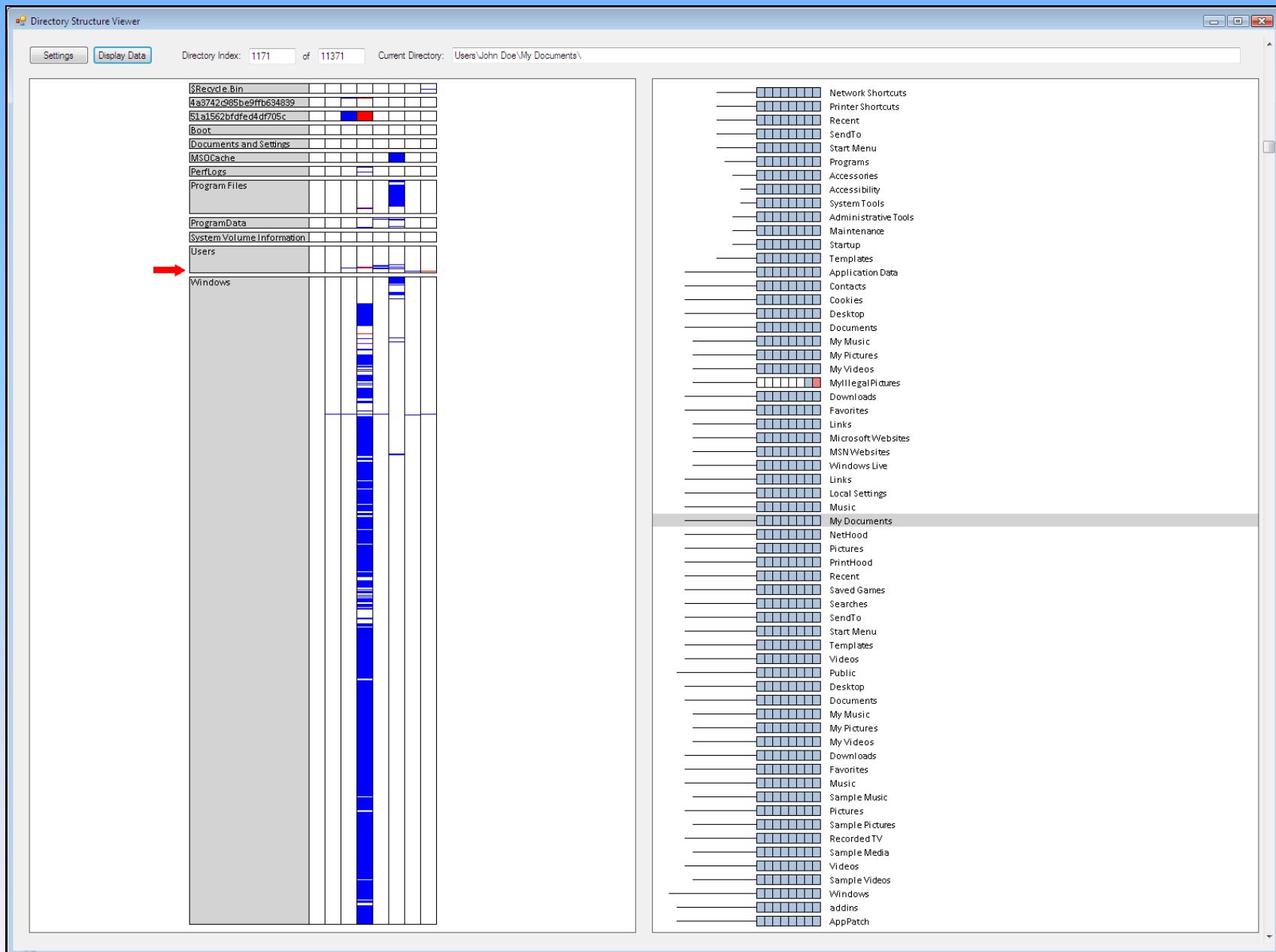


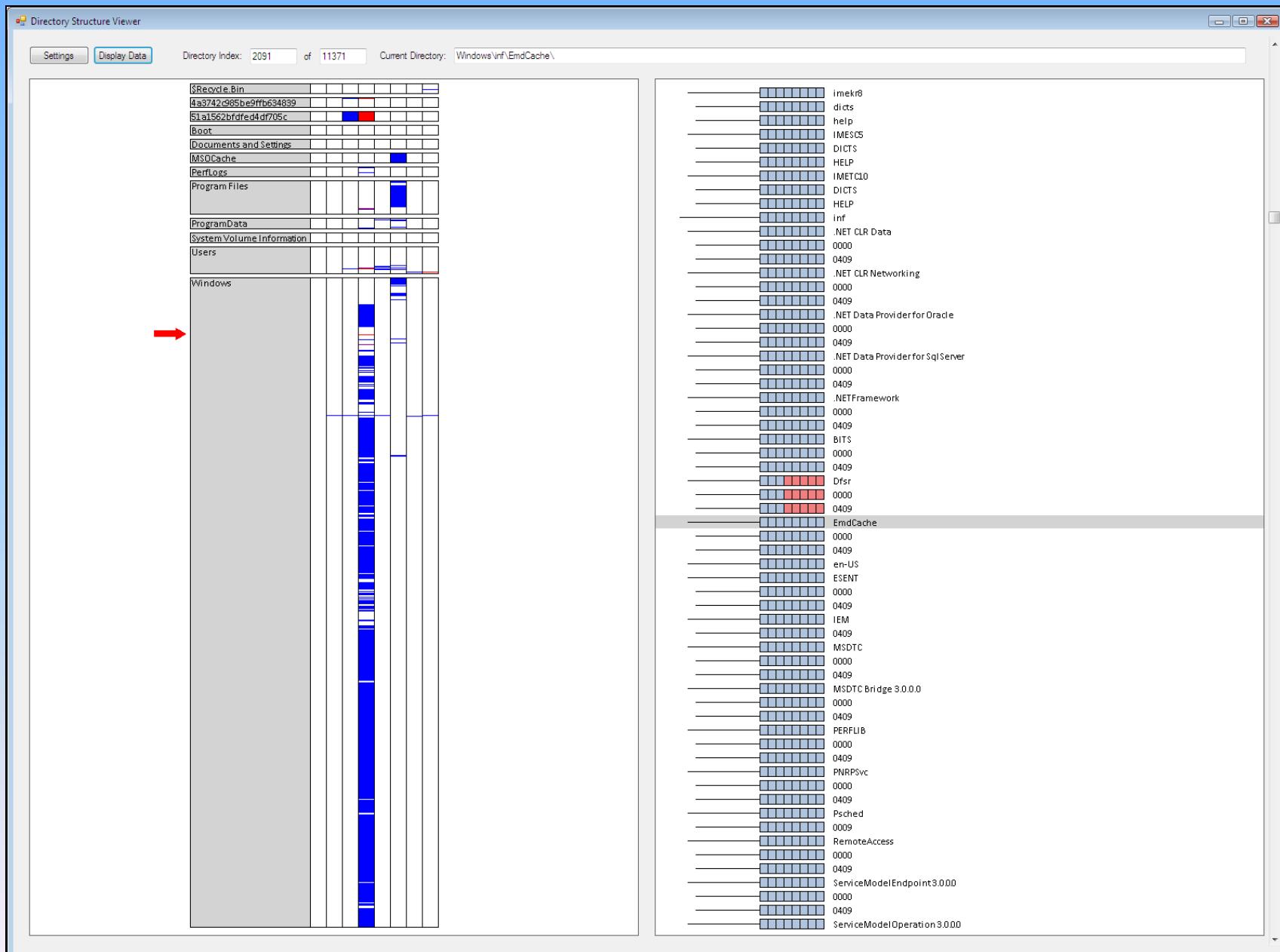


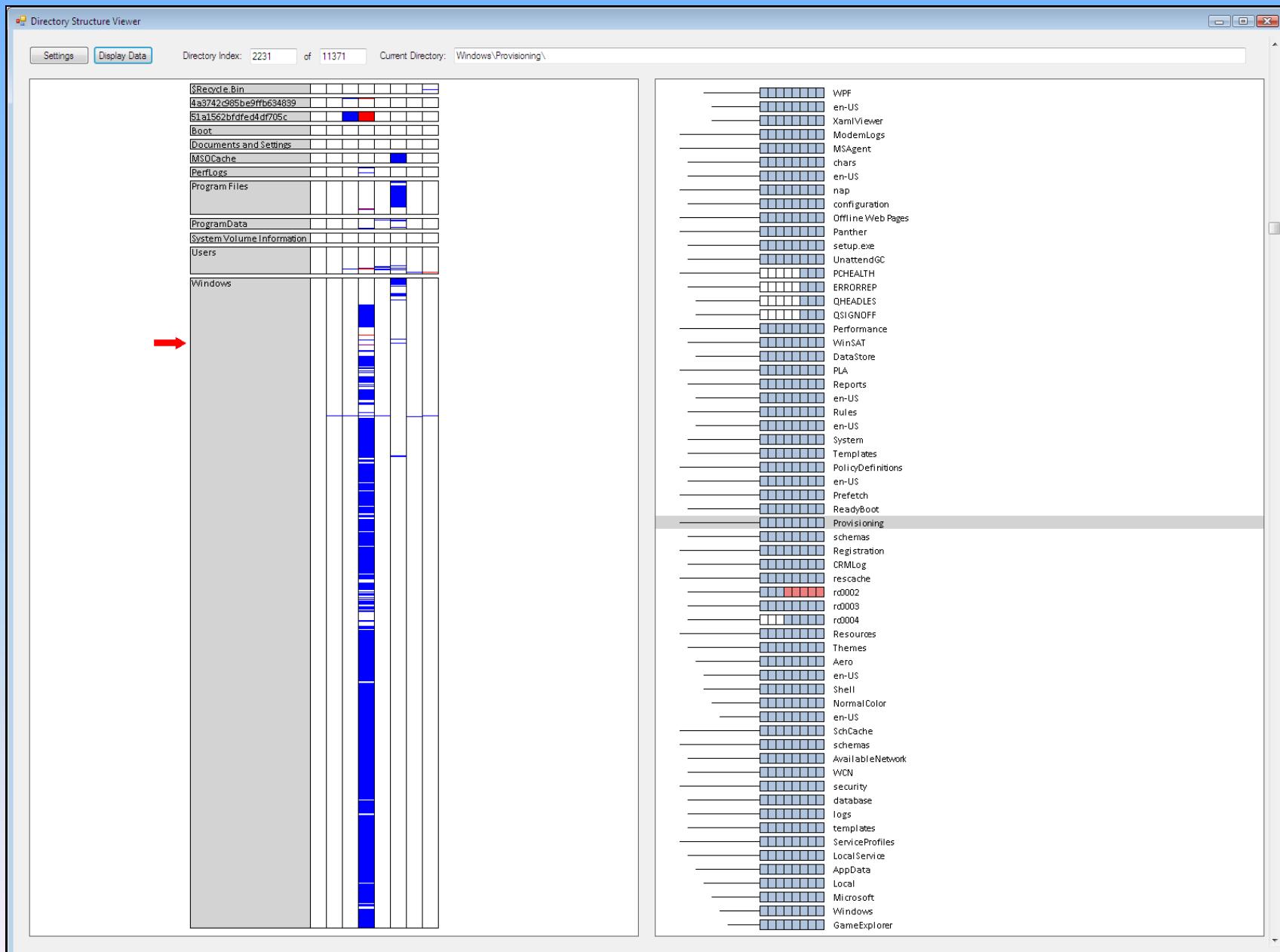




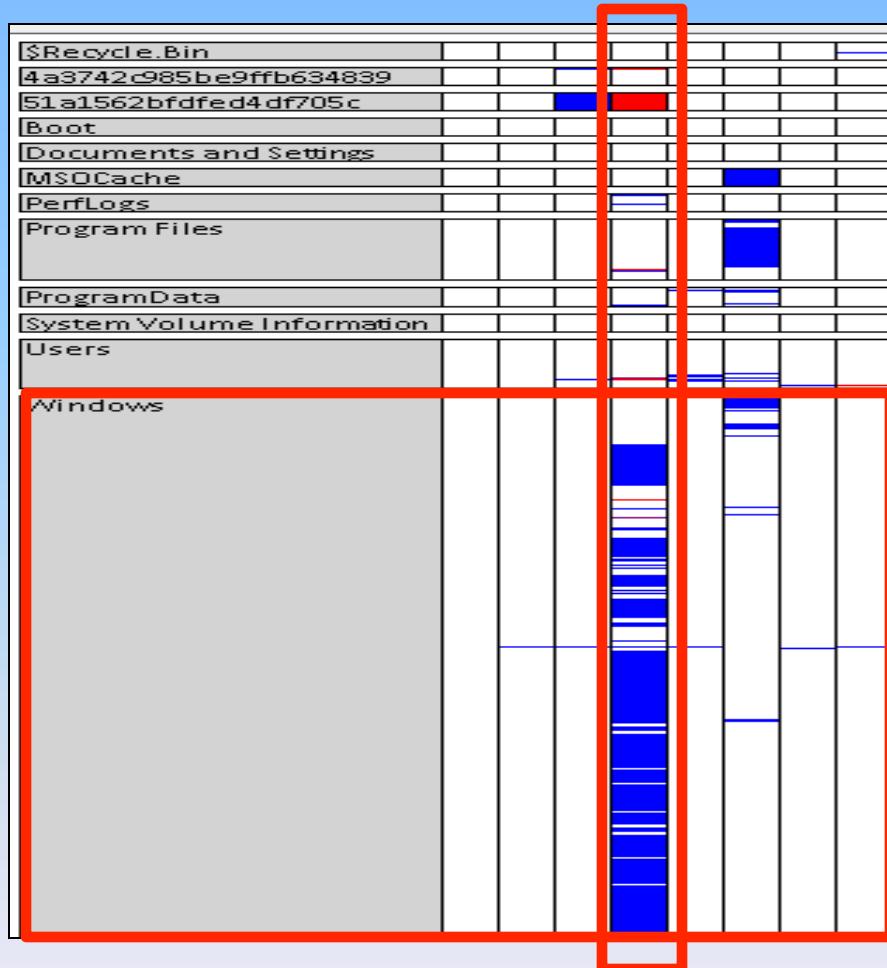






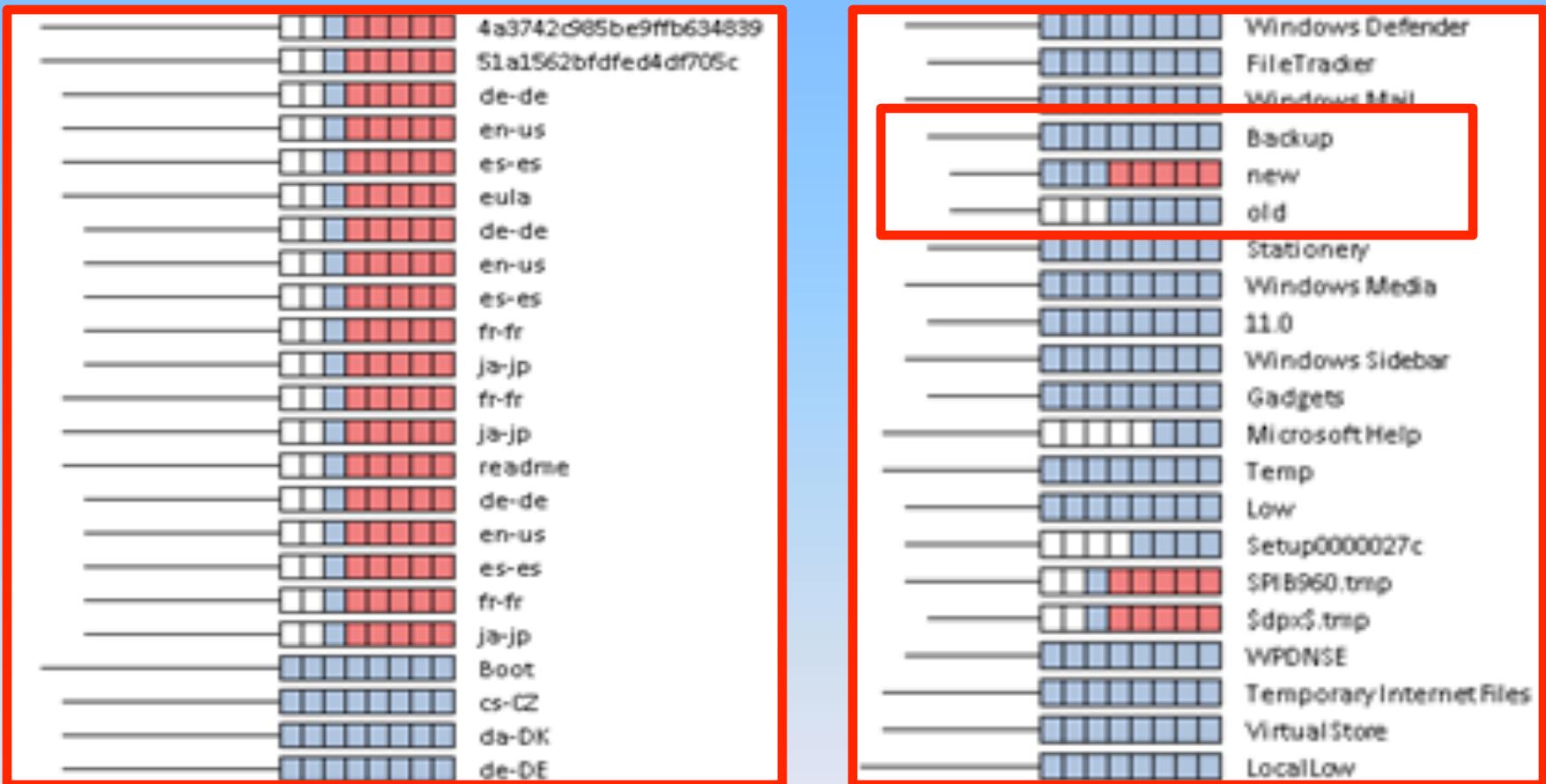


Results



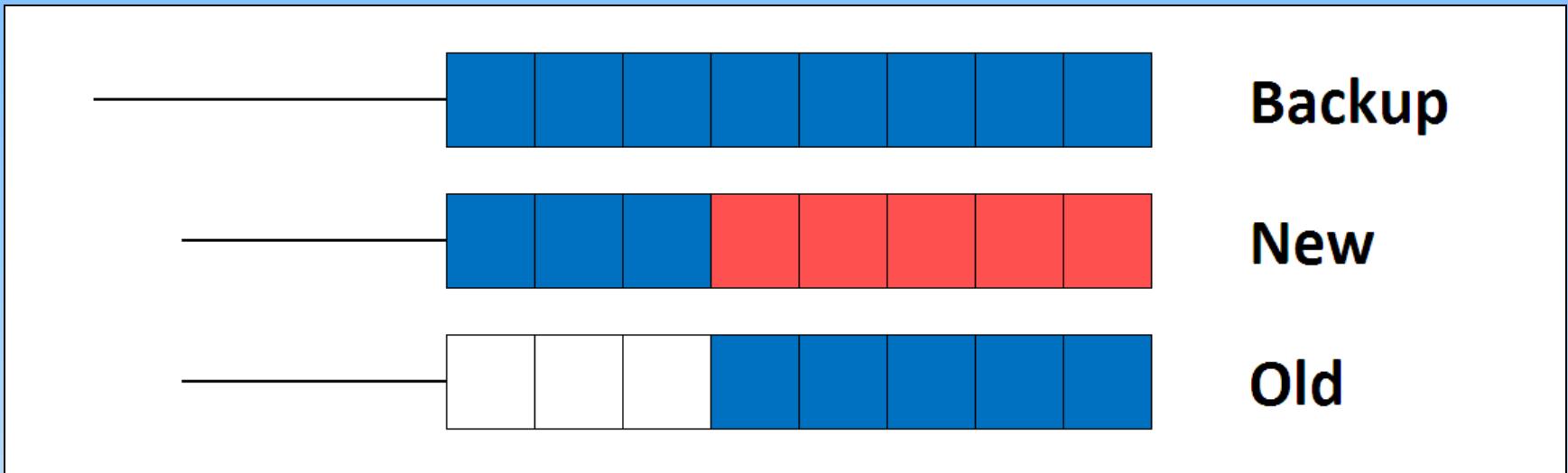
Overview of all Directory Change

Results (2)



Installation of Service Pack 1

Renaming of a Sub-Directory

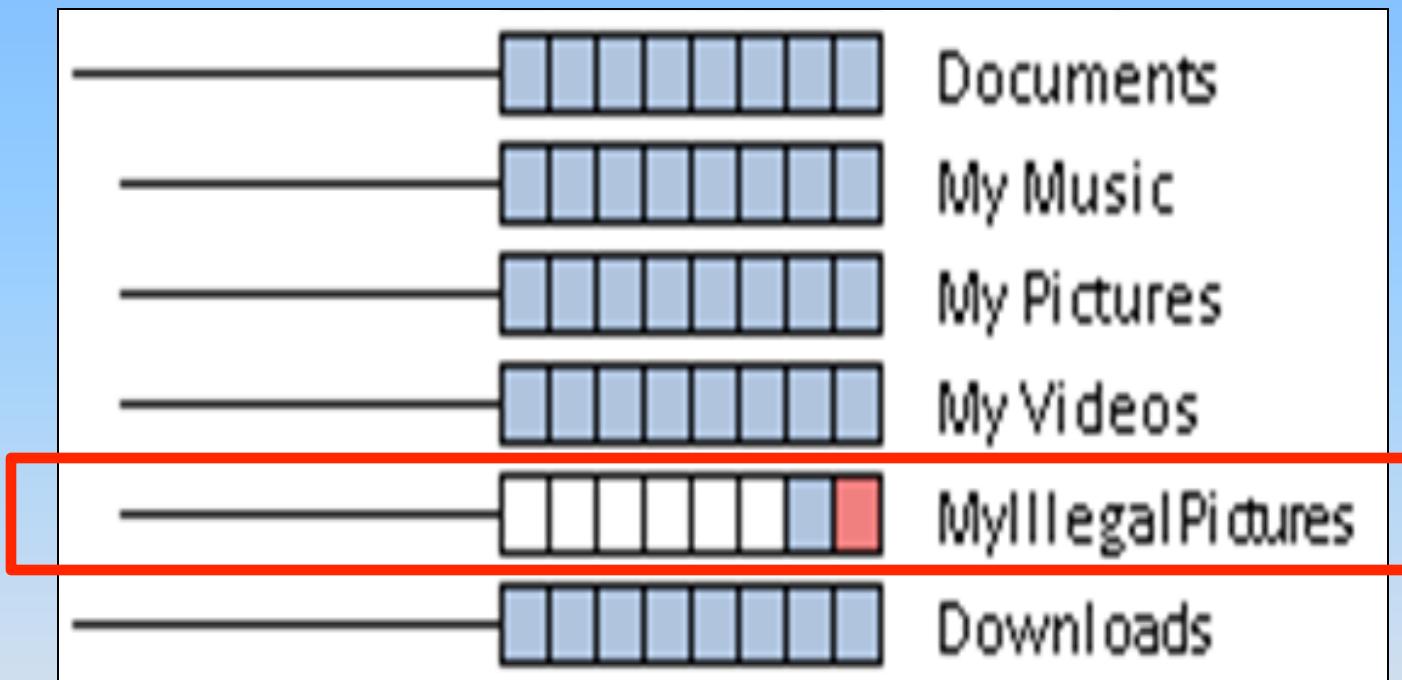


Results (3)



Activation of Vista

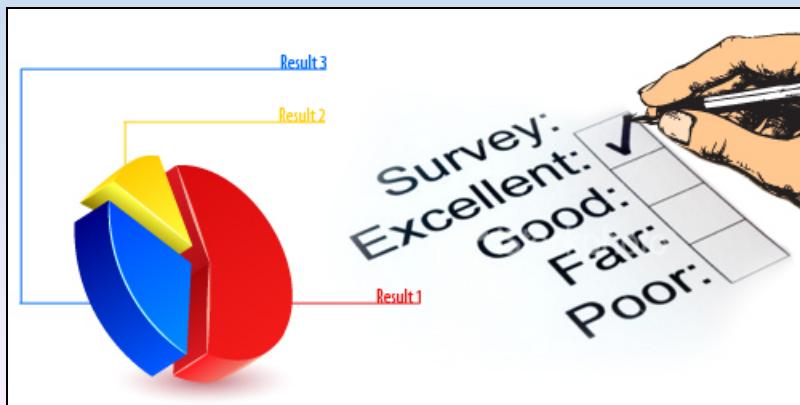
Results (4)



User Created and Deleted Directory

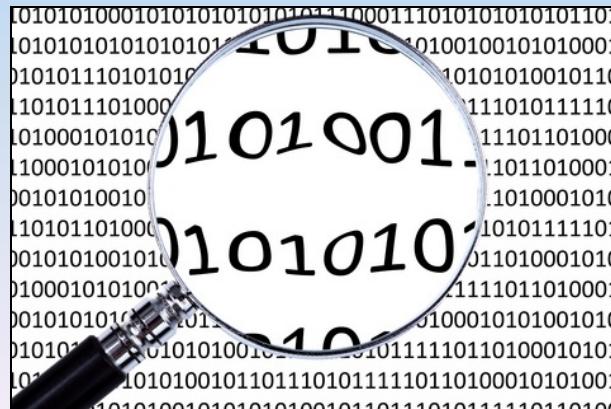
User Reactions

- Users identified periods of...
 - Most change
 - Most created directories
 - Most deleted directories
 - Root directory with the most sub-directories
- Effectiveness of segmented box and whisker glyph
- Navigation support
- Comprehension
- Color
- Whisker
- “helps understand...”
- “discover information...”



Conclusion

- Change-Link helps
 - “focus on anomalies”
 - “find meaningful data more quickly”
 - Explore data more efficiently and effectively
- Companion to existing technology
- Future Goals
 - Add two additional views:
 - Overview
 - Tree View
 - Directory View
 - File View



Thank You



<http://www.turnbacktogo.com/wp-content/uploads/2008/12/questions.jpg>