

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 that 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 computer was used to support criminal activity. Because data that have 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 box and whisker* glyph for representing change over time for individual directories, an approach for aggregating VSS data for digital forensic examinations, and a data visualization tool for exploring digital forensic data.

Categories and Subject Descriptors

H.1 [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 nonexclusive, 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 specific permission and/or a fee.

Article #12 October 13, 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. In digital forensics, the term data explosion 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 fuelled 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 subject to digital forensic examinations has 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. The repositories 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 accessing 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



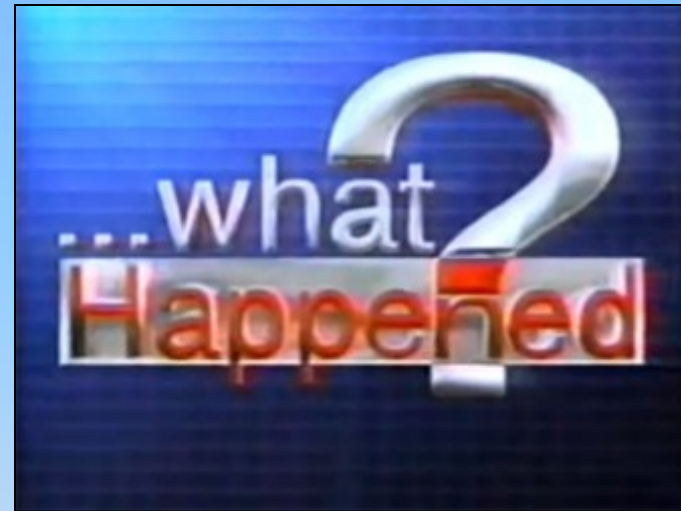
Motivation

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



Benefits of Visualizing Change

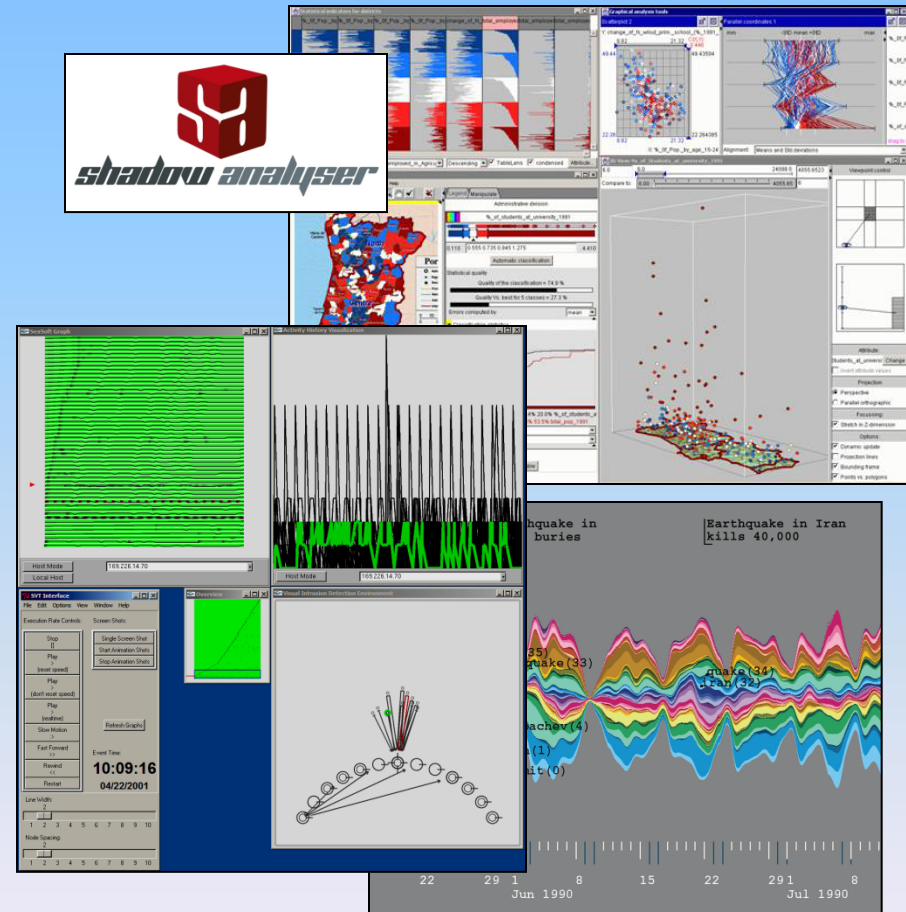
- “...direct their efforts toward more important data.”



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

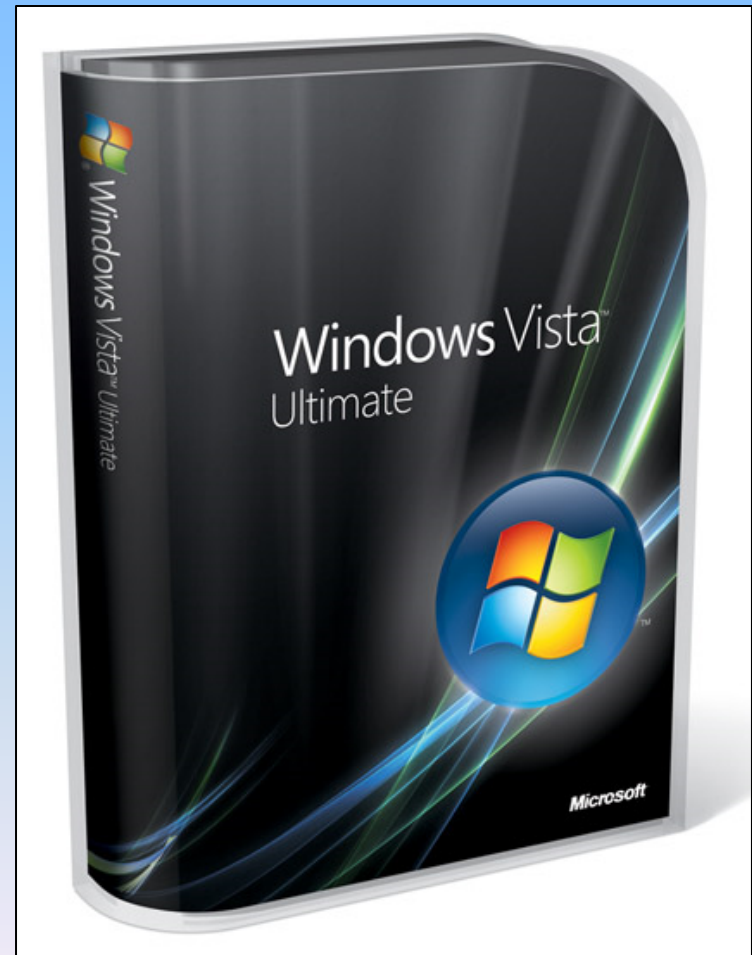
Related Work

- 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.



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.

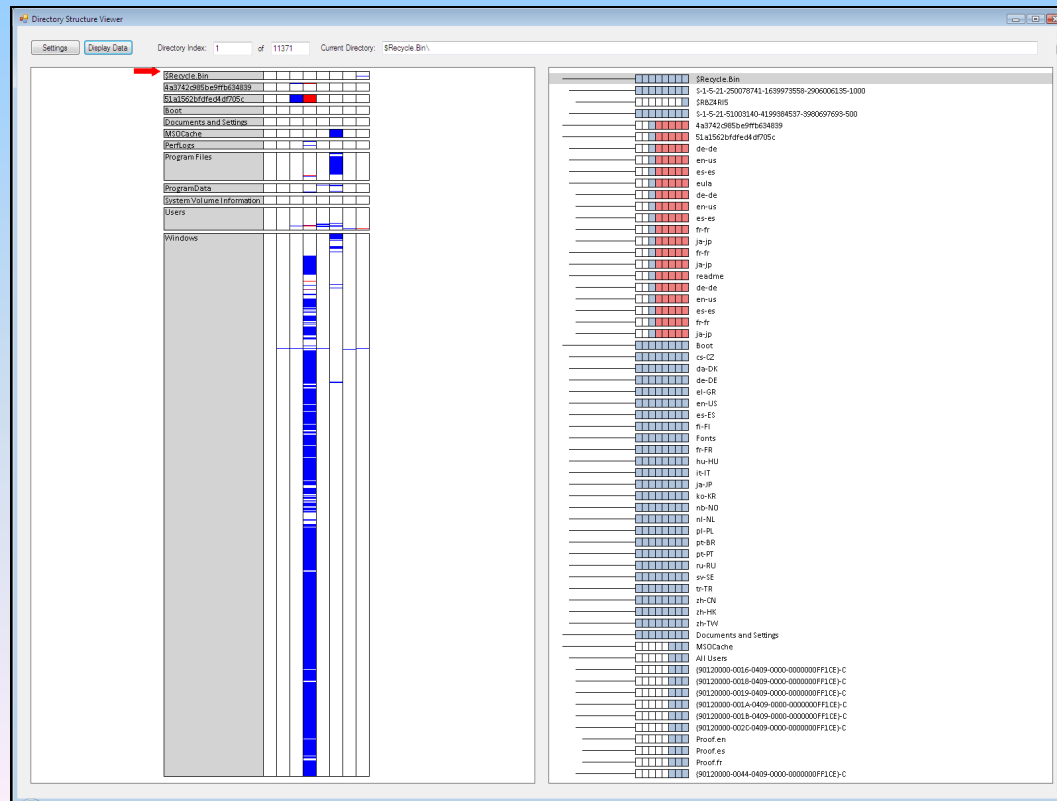
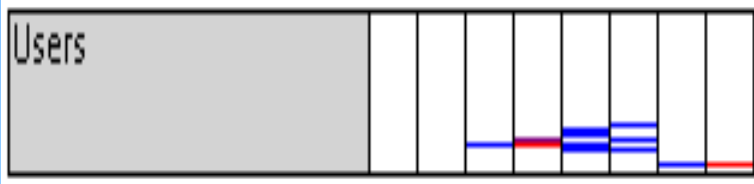


Test Data

- 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 \approx 5 million data points!



Design and Implementation



Directory Structure Viewer

Settings Display Data Directory Index: 5 of 11371 Current Directory: 4a3742c985be9fb634839\

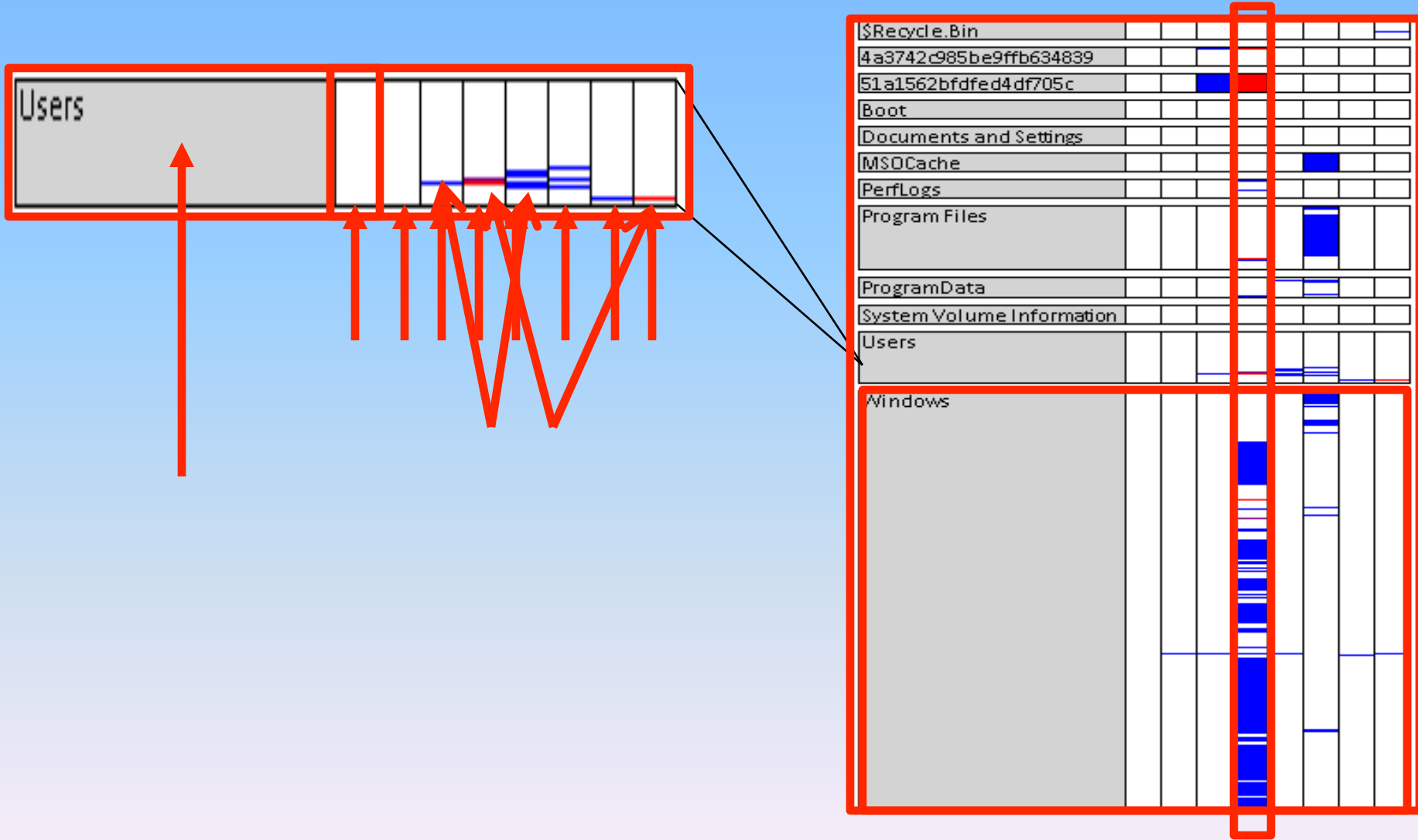
OVERVIEW

DETAIL

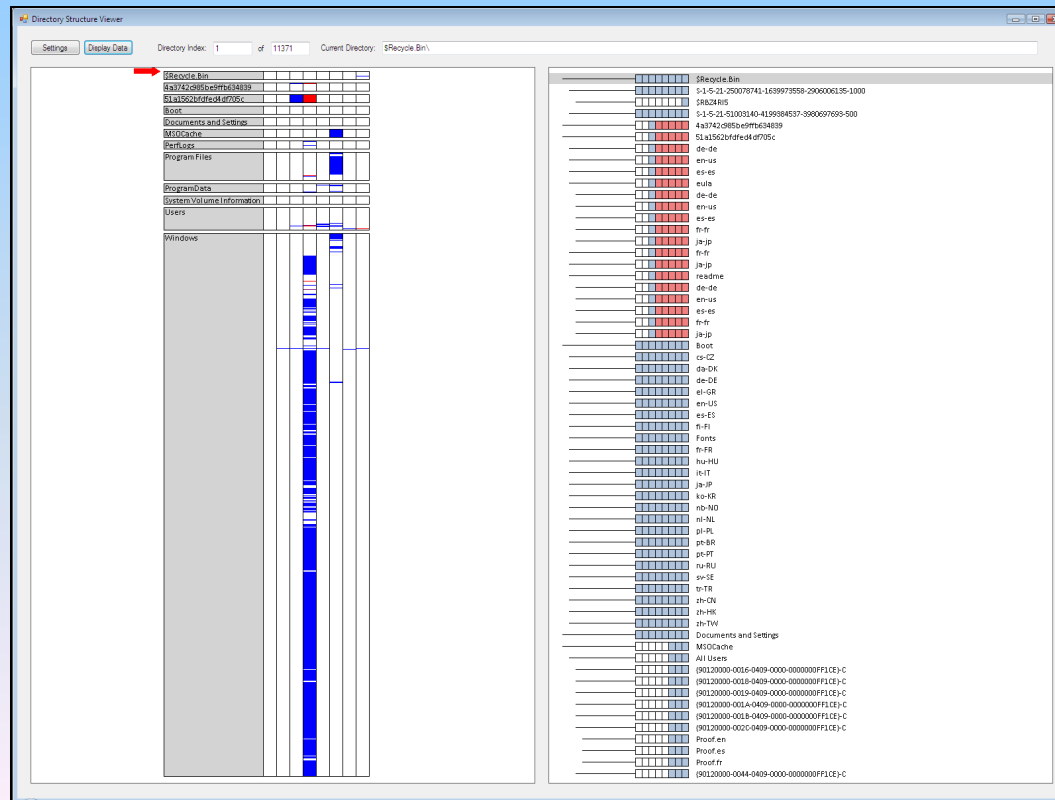
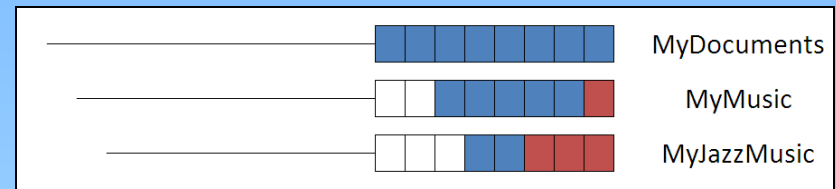
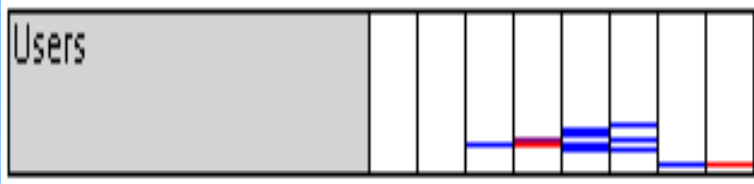
The screenshot displays the Directory Structure Viewer application. The top bar shows the current directory path: 4a3742c985be9fb634839\, with a 'Current Directory' label. Below the top bar, there are two main panels. The left panel, labeled 'OVERVIEW', shows a tree view of the directory structure. The right panel, labeled 'DETAIL', shows a list view of the directory structure. A red arrow points to the 'Display Data' button. A red circle highlights the 'Directory Index' value '5'. A red circle highlights the 'Current Directory' path. A red circle highlights the selected item in the overview view. A red circle highlights the selected item in the detail view. A red arrow points to the scroll bar on the right side of the detail view.

Item Name	Item Type
\$Recycle.Bin	Folder
4a3742c985be9fb634839	Folder
51a1562bfded4d705c	Folder
Boot	Folder
Documents and Settings	Folder
MSOCache	Folder
PerfLogs	Folder
Program Files	Folder
ProgramData	Folder
System Volume Information	Folder
Users	Folder
Windows	Folder
\$Recycle.Bin	Folder
S-1-5-21-250078741-1639973558-2906006135-1000	Folder
4a3742c985be9fb634839	Folder
S-1-5-21-51003140-4199384537-3900000000-500	Folder
4a3742c985be9fb634839	Folder
51a1562bfded4d705c	Folder
de-de	Folder
en-us	Folder
es-es	Folder
eula	Folder
de-de	Folder
en-us	Folder
fr-fr	Folder
ja-jp	Folder
ko-kr	Folder
de-de	Folder
en-us	Folder
es-es	Folder
fr-fr	Folder
ja-jp	Folder
ko-kr	Folder
nb-no	Folder
nl-nl	Folder
pl-pl	Folder
pt-br	Folder
pt-pt	Folder
ru-ru	Folder
sv-se	Folder
tr-tr	Folder
zh-cn	Folder
zh-hk	Folder
zh-tw	Folder
Documents and Settings	Folder
MSOCache	Folder
All Users	Folder
(90120000-0016-0409-0000-00000000FF1CE)-C	Folder
(90120000-0018-0409-0000-00000000FF1CE)-C	Folder
(90120000-0019-0409-0000-00000000FF1CE)-C	Folder
(90120000-001A-0409-0000-00000000FF1CE)-C	Folder
(90120000-001B-0409-0000-00000000FF1CE)-C	Folder
(90120000-002C-0409-0000-00000000FF1CE)-C	Folder
Proof.en	Folder
Proof.es	Folder
Proof.fr	Folder
(90120000-0044-0409-0000-00000000FF1CE)-C	Folder

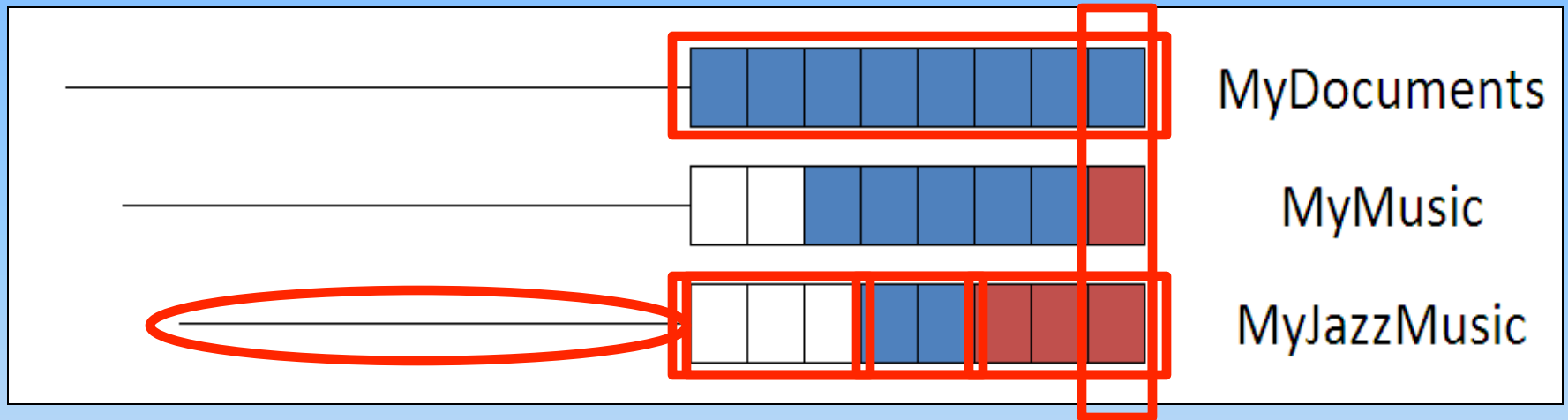
Overview Window



Design and Implementation



Segmented Box and Whisker



Directory Structure Viewer

Settings Display Data Directory Index: 1 of 11371 Current Directory: \$Recycle.Bin\

\$Recycle.Bin

4a3742c985be9ffb634839

51a1562bfded4df705c

Boot

Documents and Settings

MSOCache

PerfLogs

Program Files

ProgramData

System Volume Information

Users

Windows

\$Recycle.Bin	
\$-1-5-21-250078741-1639973558-2906006135-1000	
\$RBZARIS	
\$-1-5-21-51003140-4199984537-3980697693-500	
4a3742c985be9ffb634839	
51a1562bfded4df705c	
de-de	
en-us	
es-es	
eula	
de-de	
en-us	
es-es	
fr-fr	
ja-jp	
fr-fr	
ja-jp	
readme	
de-de	
en-us	
es-es	
fr-fr	
ja-jp	
Boot	
cs-CZ	
da-DK	
de-DE	
el-GR	
en-US	
es-ES	
fi-FI	
Fonts	
fr-FR	
hu-HU	
it-IT	
ja-JP	
ko-KR	
nb-NO	
nl-NL	
pl-PL	
pt-BR	
pt-PT	
ru-RU	
sv-SE	
tr-TR	
zh-CN	
zh-HK	
zh-TW	
Documents and Settings	
MSOCache	
All Users	
(90120000-0016-0409-0000-00000000FF1CE)-C	
(90120000-0018-0409-0000-00000000FF1CE)-C	
(90120000-0019-0409-0000-00000000FF1CE)-C	
(90120000-001A-0409-0000-00000000FF1CE)-C	
(90120000-001B-0409-0000-00000000FF1CE)-C	
(90120000-002C-0409-0000-00000000FF1CE)-C	
Proof.en	
Proof.es	
Proof.fr	
(90120000-0044-0409-0000-00000000FF1CE)-C	

Directory Structure Viewer

Settings Display Data Directory Index: 50 of 11371 Current Directory: MS0Cache\

The left pane shows a directory tree:

- \$Recycle.Bin
- 4a3742c985be9ff6634839
- 51a1562bf4fed49f705c
- Boot
- Documents and Settings
- MS0Cache
- PerfLogs
- Program Files
- ProgramData
- System Volume Information
- Users
- Windows

The right pane shows a list of files and folders:

- de-de
- en-us
- es-es
- fr-fr
- ja-jp
- Boot
- cs-CZ
- da-DK
- de-DE
- el-GR
- en-US
- es-ES
- fi-FI
- Fonts
- fr-FR
- hu-HU
- it-IT
- ja-JP
- ko-KR
- nb-NO
- nl-NL
- pl-PL
- pt-BR
- pt-PT
- ru-RU
- sv-SE
- tr-TR
- zh-CN
- zh-HK
- zh-TW
- Documents and Settings
- MS0Cache
- All Users
- (90120000-0016-0409-0000-0000000FF1CE)-C
- (90120000-0018-0409-0000-0000000FF1CE)-C
- (90120000-0019-0409-0000-0000000FF1CE)-C
- (90120000-001A-0409-0000-0000000FF1CE)-C
- (90120000-001B-0409-0000-0000000FF1CE)-C
- (90120000-002C-0409-0000-0000000FF1CE)-C
- Proof.en
- Proof.es
- Proof.fr
- (90120000-0044-0409-0000-0000000FF1CE)-C
- (90120000-00A1-0409-0000-0000000FF1CE)-C
- (90120000-0114-0409-0000-0000000FF1CE)-C
- Groove.en-us
- (90120000-0115-0409-0000-0000000FF1CE)-C
- 1033
- (90120000-0117-0409-0000-0000000FF1CE)-C
- Access.en-us
- (91120000-002E-0000-0000-0000000FF1CE)-C
- PerfLogs
- Admin
- Program Files
- Common Files
- DESIGNER
- microsoft.shared
- DAO
- DW
- EQUATION
- 1033

Directory Structure Viewer

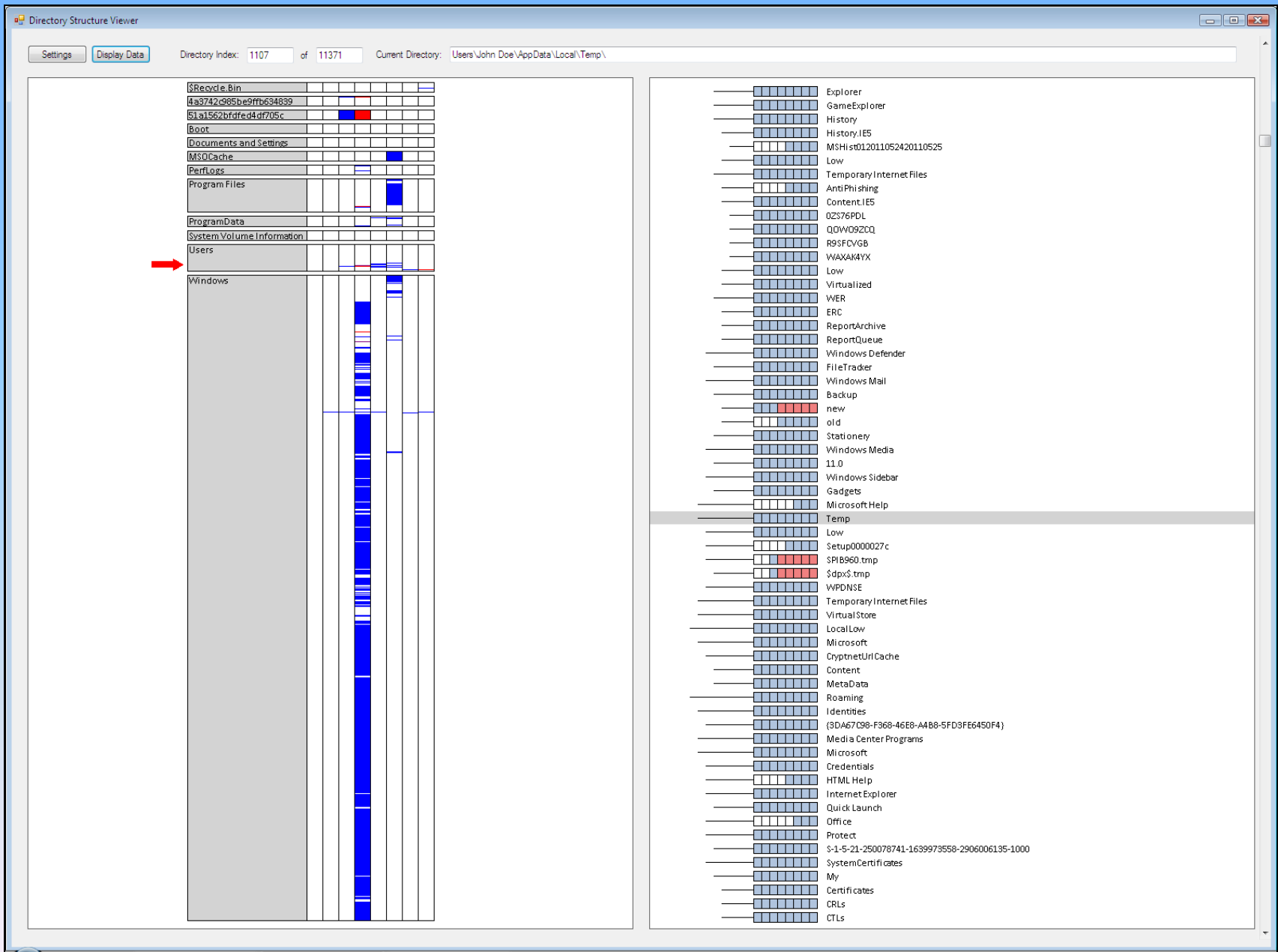
Settings Display Data Directory Index: 70 of 11371 Current Directory: PerfLogs\

Directory tree view:

- \$Recycle.Bin
- 4a3742c985be9ffb634839
- 51a1562bfafed49f705c
- Boot
- Documents and Settings
- MSOCache
- PerfLogs**
- Program Files
- ProgramData
- System Volume Information
- Users
- Windows

File list view:


- ni-NL
- pl-PL
- pt-BR
- pt-PT
- ru-RU
- sv-SE
- tr-TR
- zh-CN
- zh-HK
- zh-TW
- Documents and Settings
- MSOCache
- All Users
- (90120000-0016-0409-0000-0000000FF1CE)-C
- (90120000-0018-0409-0000-0000000FF1CE)-C
- (90120000-0019-0409-0000-0000000FF1CE)-C
- (90120000-001A-0409-0000-0000000FF1CE)-C
- (90120000-001B-0409-0000-0000000FF1CE)-C
- (90120000-002C-0409-0000-0000000FF1CE)-C
- Proof.en
- Proof.es
- Proof.fr
- (90120000-0044-0409-0000-0000000FF1CE)-C
- (90120000-00A1-0409-0000-0000000FF1CE)-C
- (90120000-0114-0409-0000-0000000FF1CE)-C
- Groove.en-us
- (90120000-0115-0409-0000-0000000FF1CE)-C
- 1033
- (90120000-0117-0409-0000-0000000FF1CE)-C
- Access.en-us
- (91120000-002E-0000-0000-0000000FF1CE)-C
- PerfLogs**
- Admin
- Program Files
- Common Files
- DESIGNER
- microsoftshared
- DAO
- DW
- EQUATION
- 1033
- EURO
- Filters
- GRPHFLT
- Help
- 1028
- 1031
- 1033
- 1036
- 1040
- 1041
- 1042
- 1046
- 1049
- 2052
- 3082
- ink
- 1.0
- 1.7
- ar-SA
- bg-BG



Directory Structure Viewer

Settings Display Data Directory Index: 1171 of 11371 Current Directory: Users\John Doe\My Documents\

\$Recycle Bin							
4a3742c985be9ffb634839							
51a1562bfdred4d705c							
Boot							
Documents and Settings							
MSOCache							
PerfLogs							
Program Files							
ProgramData							
System Volume Information							
Users							
Windows							




- Network Shortcuts
- Printer Shortcuts
- Recent
- SendTo
- Start Menu
- Programs
- Accessories
- Accessibility
- System Tools
- Administrative Tools
- Maintenance
- Startup
- Templates
- Application Data
- Contacts
- Cookies
- Desktop
- Documents
- My Music
- My Pictures
- My Videos
- My Recent Places
- Downloads
- Favorites
- Links
- Microsoft Websites
- MSN Websites
- Windows Live
- Links
- Local Settings
- Music
- My Documents
- NetHood
- Pictures
- PrintHood
- Recent
- Saved Games
- Searches
- SendTo
- Start Menu
- Templates
- Videos
- Public
- Desktop
- Documents
- My Music
- My Pictures
- My Videos
- Downloads
- Favorites
- Music
- Sample Music
- Pictures
- Sample Pictures
- Recorded TV
- Sample Media
- Videos
- Sample Videos
- Windows
- addins
- AppPatch

Directory Structure Viewer

Settings Display Data Directory Index: 2091 of 11371 Current Directory: Windows\inf\EmdCache\

\$Recycle.Bin								
4a3742c985be9ff634839								
51a1562bfafed49f705c								
Boot								
Documents and Settings								
MSDCache								
PerfLogs								
Program Files								
ProgramData								
System Volume Information								
Users								
Windows								




										imekr8
										dicts
										help
										IMESCS
										DICTS
										HELP
										IMETCLO
										DICTS
										HELP
										inf
										.NET CLR Data
										0000
										0409
										.NET CLR Networking
										0000
										0409
										.NET Data Provider for Oracle
										0000
										0409
										.NET Data Provider for Sql Server
										0000
										0409
										.NETFramework
										0000
										0409
										BITS
										0000
										0409
										Dfsr
										0000
										0409
										EmdCache
										0000
										0409
										en-US
										ESENT
										0000
										0409
										IEM
										0409
										MSDTC
										0000
										0409
										MSDTC Bridge 3.0.0.0
										0000
										0409
										PERFLIB
										0000
										0409
										PNRPsvc
										0000
										0409
										Psched
										0009
										RemoteAccess
										0000
										0409
										ServiceModelEndpoint3.0.0
										0000
										0409
										ServiceModelOperation3.0.0

Directory Structure Viewer

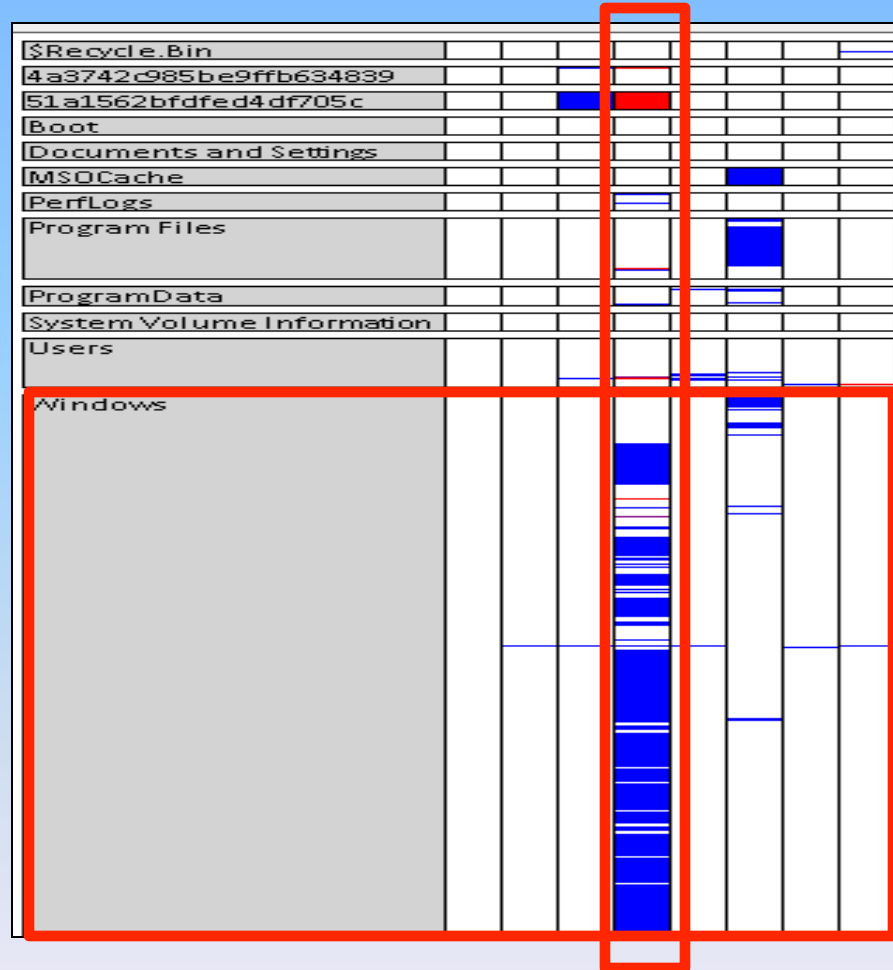
Settings Display Data Directory Index: 2231 of 11371 Current Directory: Windows\Provisioning\

\$Recycle.Bin					
4a3742c985be9ffb634839					
51a1562bfafed49f705c					
Boot					
Documents and Settings					
MSOCache					
PerfLogs					
Program Files					
ProgramData					
System Volume Information					
Users					
Windows					



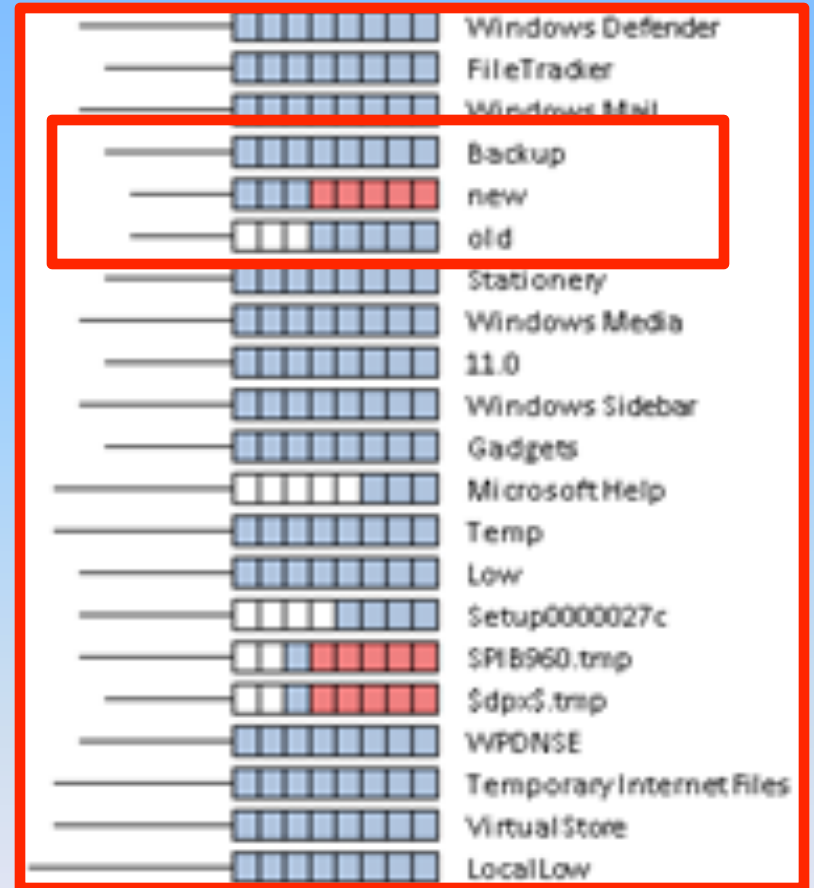
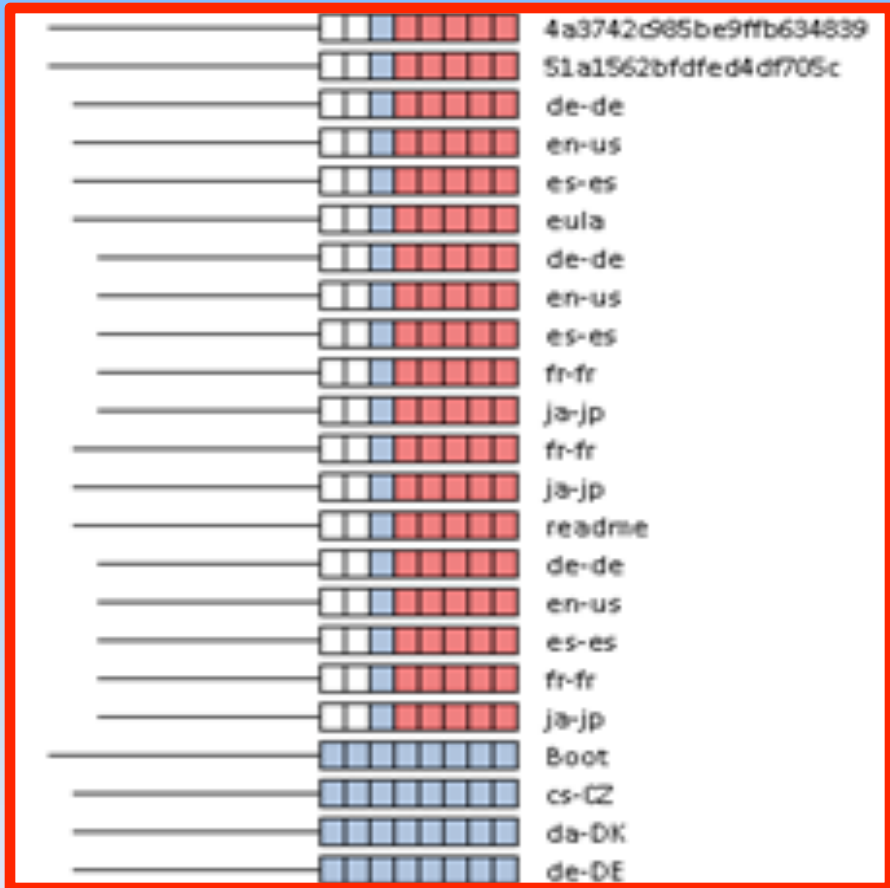
WFF					
en-US					
XamlViewer					
ModemLogs					
MSAgent					
chars					
en-US					
nap					
configuration					
OfflineWebPages					
Panther					
setup.exe					
UnattendGC					
PCHEALTH					
ERRORREP					
QHEADLES					
QSIGNOFF					
Performance					
WinSAT					
DataStore					
PLA					
Reports					
en-US					
Rules					
en-US					
System					
Templates					
PolicyDefinitions					
en-US					
Prefetch					
Readyboot					
Provisioning					
schemas					
Registration					
CRMLog					
rescache					
rd002					
rd003					
rd004					
Resources					
Themes					
Aero					
en-US					
Shell					
Normal Color					
en-US					
SchCache					
schemas					
AvailableNetwork					
WCN					
security					
database					
logs					
templates					
ServiceProfiles					
LocalService					
AppData					
Local					
Microsoft					
Windows					
GameExplorer					

Results



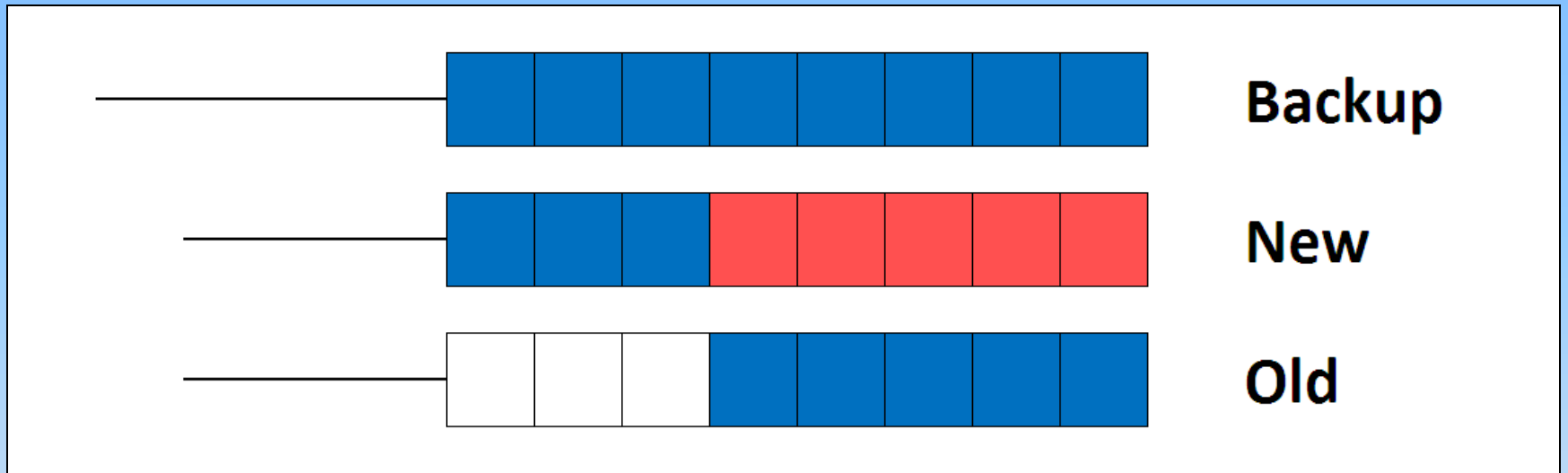
Overview of all Directory Change

Results (2)

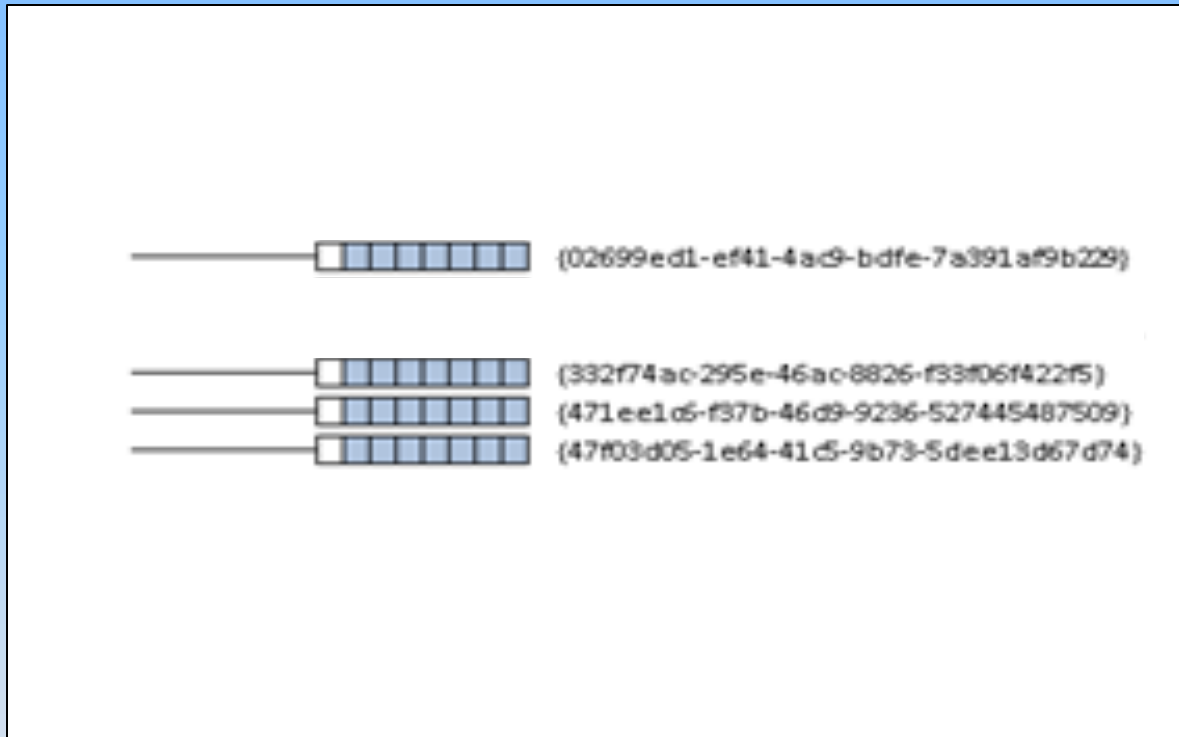


Installation of Service Pack 1

Renaming of a Sub-Directory

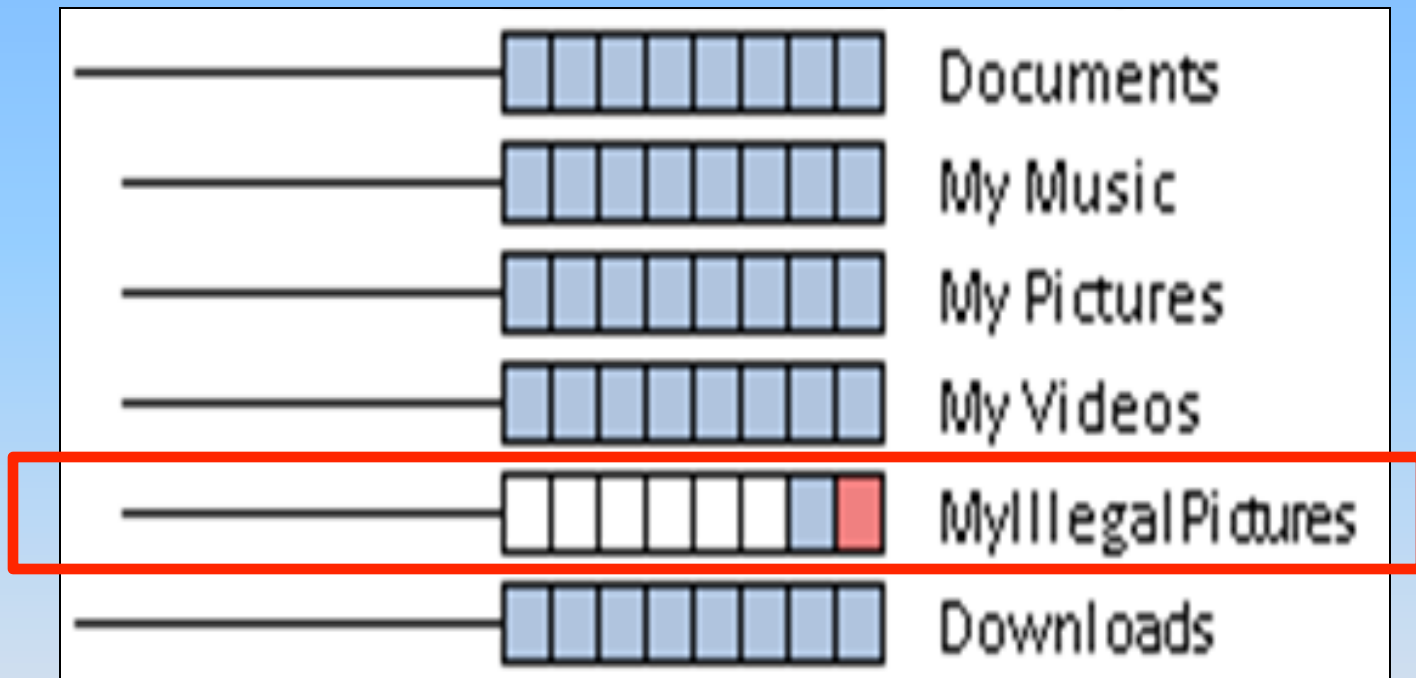


Results (3)



Activation of Vista

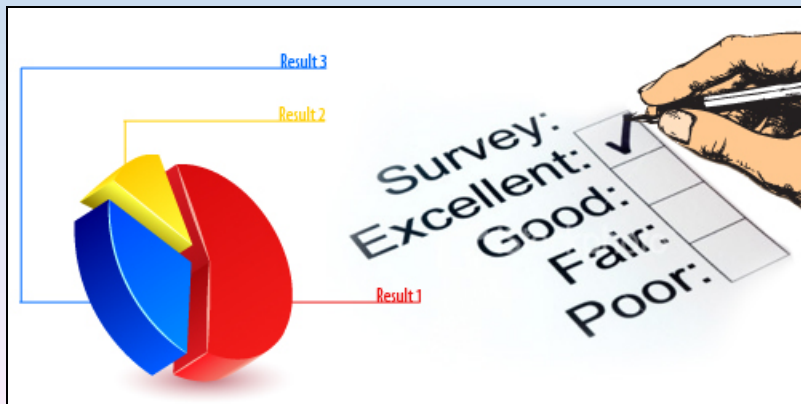
Results (4)



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.turnbacktgod.com/wp-content/uploads/2008/12/questions.jpg>