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

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.

http://home.comcast.net/~SupportCD/Images/Windows_Vista_Ultimate_Box_HiRes.jpg
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

DETAIL
Overview Window
Design and Implementation
Segmented Box and Whisker

MyDocuments
MyMusic
MyJazzMusic
Results

Overview of all Directory Change
Installation of Service Pack 1
Renaming of a Sub-Directory

Backup

New

Old
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…”

http://www.experiment-resources.com/images/survey-research-design.jpg
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