Different Interpretations of ISO9660 File Systems

By

Brian Carrier

Presented At

The Digital Forensic Research Conference

DFRWS 2010 USA Portland, OR (Aug 2nd - 4th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Different Interpretations of ISO9660 File Systems

Brian Carrier

©2010, Basis Technology.

Basis Technology Corporation

P 617.386.2000
800.697.2062 (toll-free)
F 617.386.2020
W info@basistech.com
www.basistech.com

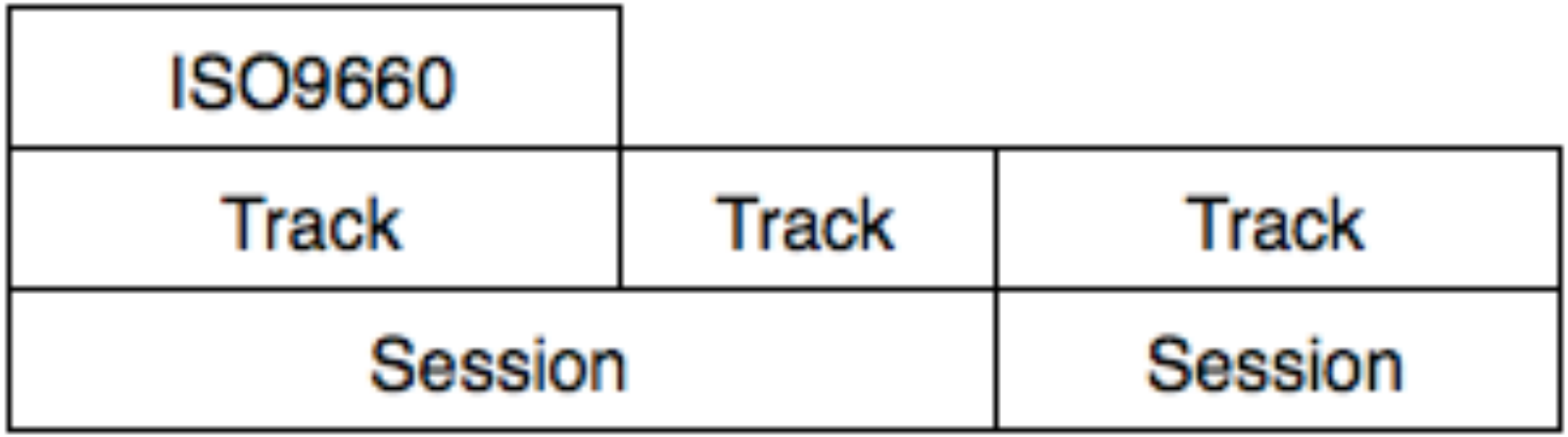
Agenda

- Basics of ISO9660
- Test Description and Results

©2010, Basis Technology.

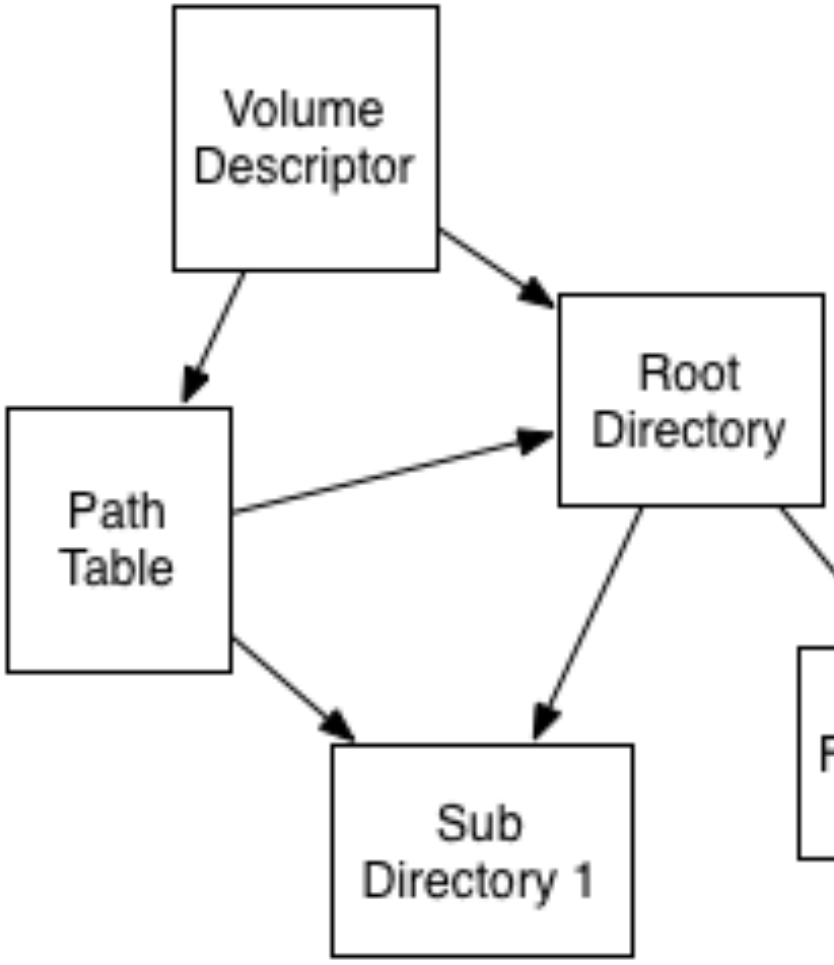
Sessions vs. File Systems

- A physical CD can have one or more sessions.
- A session can have one or more tracks.
- A track can contain an ISO9660 file system.



©2010, Basis Technology.

Very High Level Overview



- **Volume Descriptor** is located at fixed offset in the beginning of the FS.
- **Path Table** has an entry for each directory in FS.
- **Directories** contain a list of entries. One for each of its files and sub-directories.

©2010, Basis Technology.

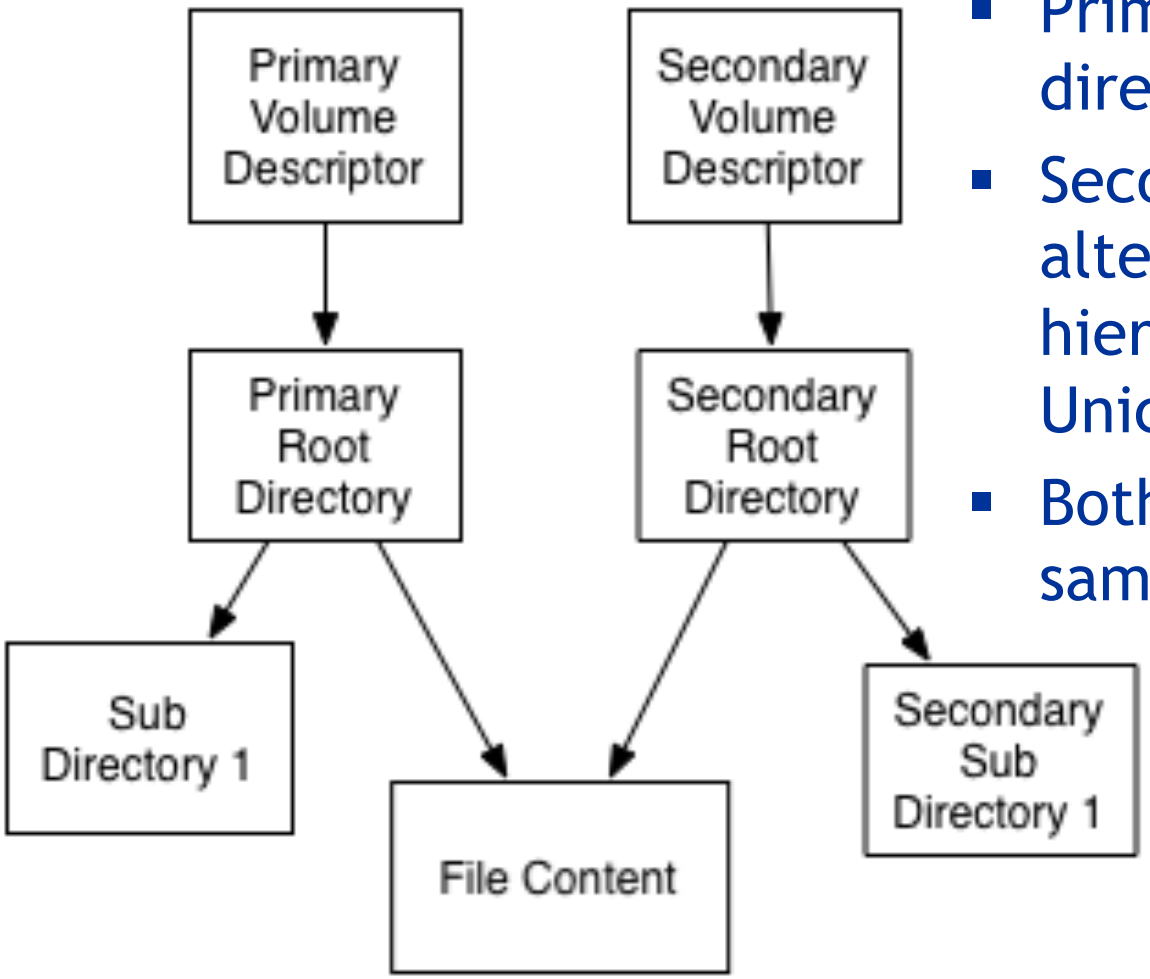
Basic Limitations

- File names are restricted to 8 characters in the name and 3 in the extension.
- Use of non-English file names is limited.
- Solution:
  - Create a separate directory hierarchy and store alternative forms of file names in it.
  - Joliet extension allows for longer names in Unicode.

BASIS TECHNOLOGY

©2010, Basis Technology.

Multiple Volume Descriptors



- Primary points to 8.3 directory hierarchy.
- Secondary points to alternative directory hierarchies (i.e. Joliet / Unicode)
- Both can refer to the same file content.

©2010, Basis Technology.

File Content

- Files on a CD are, generally, not fragmented.
  - Some have a consistent and defined interleave
- Location of file content is specified with only two values:
  - Starting block address
  - File size

©2010, Basis Technology.

Endian Ordering

- File systems generally store data in a single endian byte ordering:
  - Big Endian: `12 34 56 78`
  - Little Endian: `78 56 34 12`
- ISO9660 stores most of its values in both big and little endian ordering:
  - FS block sizes and block count
  - File size and starting block location
  - …

BASIS TECHNOLOGY

©2010, Basis Technology.

ISO9660 Interpretations

- The design of ISO9660 allows for multiple interpretations:
  - Multiple directory hierarchies
  - Multiple endian orderings
- If a forensic tool chooses only one of multiple interpretations, then it may miss evidence.
- This work created disk images to test what interpretations that the tools were choosing.
- Test images will be made available at

  http://dftt.sf.net

BASIS TECHNOLOGY

©2010, Basis Technology.

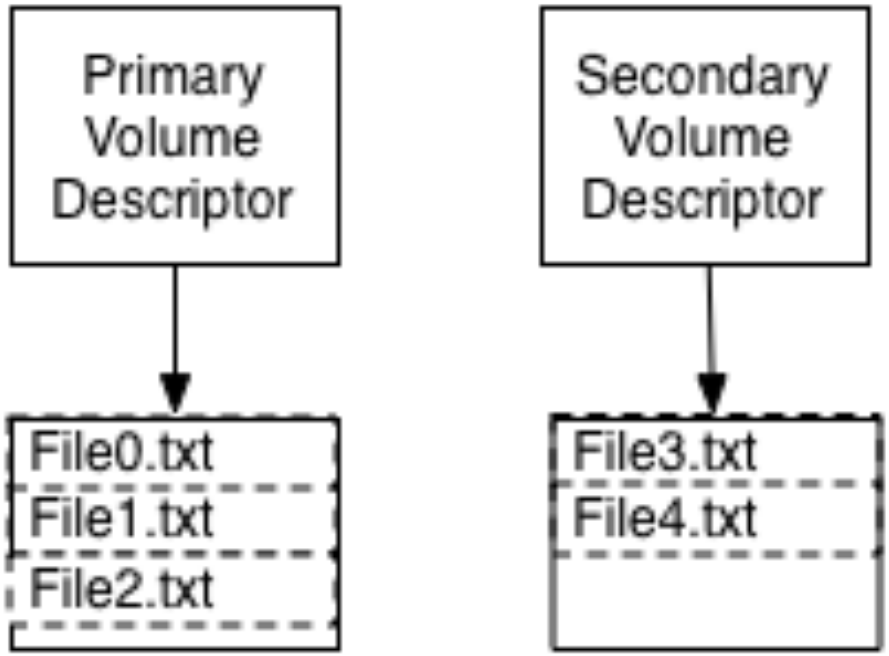
Tools Tested

- Import disk image file:
  - EnCase 6.15
  - Forensic Tool Kit (FTK) 1.60
  - ISOBuster 2.7
  - Sleuth Kit (TSK) 3.1.0
  - WinHex Forensics: With and without “Read ISO9660 even if Joliet Present” option.
- Linux 2.6: Physical CD and mounted disk image in loopback:
  - Default options
  - Nojoliet option
  - Norock option
- OS X 10.4.11 (Power PC) and OS X 10.6.2 (Intel): Physical CD and mounted disk image with Disk Utility
- Windows XP and Vista: Physical CD

©2010, Basis Technology.

Test #1: Inconsistent Directories

- There is no requirement that the multiple directory hierarchies are consistent.
- Test: Place different files in each root directory and see what is displayed in each tool.



©2010, Basis Technology.

Test #1 Creation

- Create a Joliet image with two files in root directory: File1.txt and File2.txt.
- Used fsstat in TSK to locate the primary and secondary root directories.
- Used hex editor to:
  - Zero out the File2.txt entry in the primary hierarchy.
  - Overwrite the File1.txt entry in the secondary hierarchy with the File2.txt entry.

©2010, Basis Technology.

Test #1 Results

- Displayed both files:
  - FTK
  - ISOBuster
  - TSK
  - WinHex Forensics ("Read ISO9660 even if Joliet Present" option enabled)
- Displayed only File1 (Primary Descriptor):
  - Linux (via CD, default mount options, nojoliet options)
  - OS X (via CD, Disk Utility mount)

©2010, Basis Technology.

Test #1 Results (contd.)

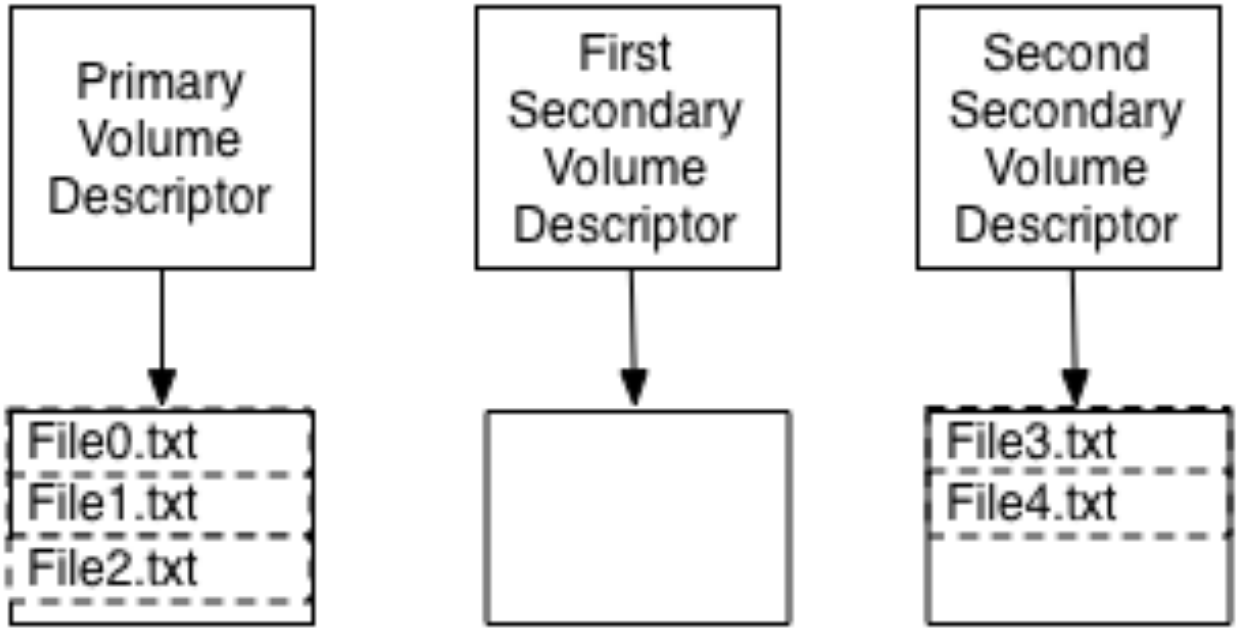
- Displayed only File2 (Secondary Descriptor):
  - EnCase
  - Linux (norock mount option)
  - Windows XP and Vista
  - WinHex Forensics (default options)
- Summary:
  - 28% showed both files
  - 36% showed only File1.txt
  - 36% showed only File2.txt

BASIS TECHNOLOGY

©2010, Basis Technology.

Test #2: Three Hierarchies

- Several of the tools seem to look only at the second hierarchy.
- Test: Have three hierarchies with the second one being empty and different files in others.



©2010, Basis Technology.

Test #2 Creation

- Started with image from Test #1.
- Manually created third hierarchy using the second one as a base:
  - Used ‘blkls’ in TSK to identify unused blocks to store new root directory and path table.
  - Copied existing root directory and path table into them.
  - Copied existing secondary volume descriptor to make the second secondary descriptor and adjusted root directory and path table values.
- Zeroed out contents of second root directory.

©2010, Basis Technology.

Test #2 Results

- Showed both File1.txt and File2.txt (same as test #1):
  - FTK, ISOBuster, TSK, WinHex Forensics (with ISO9660 option)
- Showed only File1.txt (same as test #1):
  - Linux (CD, default mount, nojoliet mount), OS X
- Showed only File2.txt (subset of test #1):
  - WinHex Forensics (default options)
- Showed no files:
  - EnCase, Linux (norock option), Windows XP and Vista
- Summary:
  - 28.5% showed both files
  - 36% showed only File1.txt
  - 7% showed only File2.txt
  - 28.5% showed no files

BASIS TECHNOLOGY

©2010, Basis Technology.

Test #3: Endian Ordering

- Many values are stored in both big- and little-endian orderings.
- Test: Have a file with different starting block address values in the different orderings.

Name	Starting Block (big-endian)	Starting Block (little-endian)
File1.txt	00 00 00 20	30 00 00 00

BASIS TECHNOLOGY

©2010, Basis Technology.

Test #3 Creation

- Create an image with a single file whose contents are “This tool uses the little-endian value”.
- Locate the root directory and file contents using TSK.
- Copy the file contents to a free block and edit with a hex editor to have “This tool uses the big-endian value”.
- Edit the file entry so that its big-endian starting block value is the above block.

©2010, Basis Technology.

Test #3 Results

- Displays Both Files:
  - ISOBuster (with non-default settings)
- Displays Big Endian:
  - FTK, ISOBuster (with default settings), TSK
- Displays Little Endian:
  - EnCase, Linux (all variations), OS X (all variations and platforms), Windows (all variations), WinHex (all variations)
- Summary:
  - 6% show both values
  - 19% use only big-endian value
  - 75% use only little-endian value
  - 0% report any type of warning

BASIS TECHNOLOGY

©2010, Basis Technology.

Test Summary

- Many tools choose only one interpretation:
  - 72% show only one file in the first two tests.
  - 65% don't look beyond the first secondary descriptor
  - 29% failed to show either file in test 2
  - None of the tools warned about inconsistent endian ordering values.
- The tools are not consistent about which interpretation they choose

©2010, Basis Technology.

Data Hiding Implications

- These techniques could work, but it would be risky because some of the tools may show the hidden files.
- The file content can still be found from carving and keyword searching unallocated space.

©2010, Basis Technology.

Recommendation

- Use one of the tools that considers multiple interpretations.
- Use multiple tools that consider different interpretations.
  - Somehow merge the results together…
- Urge the tool vendors to consider multiple interpretations.

©2010, Basis Technology.

User Interface Challenge

- ISO9660 is so different from typical file systems that it creates an interface challenge.
- How to show multiple directory hierarchies in the analysis tool?
  - FTK, ISOBuster, and WinHex showed each of the hierarchies in their entirety.
  - TSK showed the Secondary descriptor as the default hierarchy and showed files from the other hierarchies as orphan files that could not be reached from the root directory.
- How to show keyword search results when a file has a different path in each hierarchy (show it as one hit or two)?
- How to allow user to view both big- and little-endian interpretation of the data?

BASIS TECHNOLOGY

©2010, Basis Technology.

Possible Future Work

- Analyze popular disk mastering software to determine if they use techniques similar to these:
  - Maybe different endian values are used to refer to endian-specific file content.
  - Could help to evaluate if existence of these techniques on a CD implies malicious intent.
- Define a standard procedure for analyzing ISO9660 file systems.

BASIS TECHNOLOGY

©2010, Basis Technology.

Brian Carrier

brianc <at> basistech <dot> com

©2010, Basis Technology.