SANS DFIR Summit 2019

.DS_Stores: Like Shellbags but for Macs

NICOLE IBRAHIM

KPMG, LLP

Who am I

- Senior Associate, Cyber Response at KPMG, LLP
- Forensics
- Researcher
- Programmer

Nicole Ibrahim | Senior Associate, Cyber Response | KMPG, LLP

nicoleibrahim@kpmg.com | @nicoleibrahim

Importance

- Additional artifact source for folder accesses
- Reveals how a folder was accessed
- Requires Finder GUI interaction
- Currently underutilized

Agenda

- Introduction to .DS_Stores
- Parsing .DS_Stores
- Understanding parsed data
- Limitations and caveats

Introduction to .DS_Stores

Introduction to .DS_Stores

- Desktop Services Store
- MacOS Finder GUI application
- Around since OSX Tiger 10.4
- Contains custom view settings on a per folder basis
- On a fresh install of MacOS, only three of these exist by default:
  - /.DS_Store
  - /Applications/.DS_Store
  - /Applications/Utilities/.DS_Store

Introduction to .DS_Stores
Where are they located?

- Can be found in any folder on any File System
- Accessed using Finder
- A user has write permissions to
- Can include:
  - Internal drives
  - External drives
  - Network shares

Introduction to .DS_Stores
Why are they created?

- Various ways these files can be created and/or modified.
- All require user interaction. Some examples include:
  - The view style was changed
  - The Finder window size/location/scroll position has change
  - A folder is double-clicked in Finder
  - A folder is expanded while in “List View”
  - A folder is right-clicked and “Open in new Tab” is selected

Introduction to .DS_Stores
What do they Contain?

- Each .DS_Store can have multiple records
- A file/folder can have multiple entries in a .DS_Store
- Data is stored in b-tree format

Name	• The name in unicode of the file/folder the record pertains to.
Record Type	• A four letter string code indicating the record entry type.
Data Format	• A four letter string code indicating the format of the record data.
Record Data	• The record data. Used by Finder to display customized view settings.

- The file format is covered here: https://metacpan.org/pod/distribution/Mac-Finder-DSStore/DSStoreFormat.pod#FILE-FORMAT

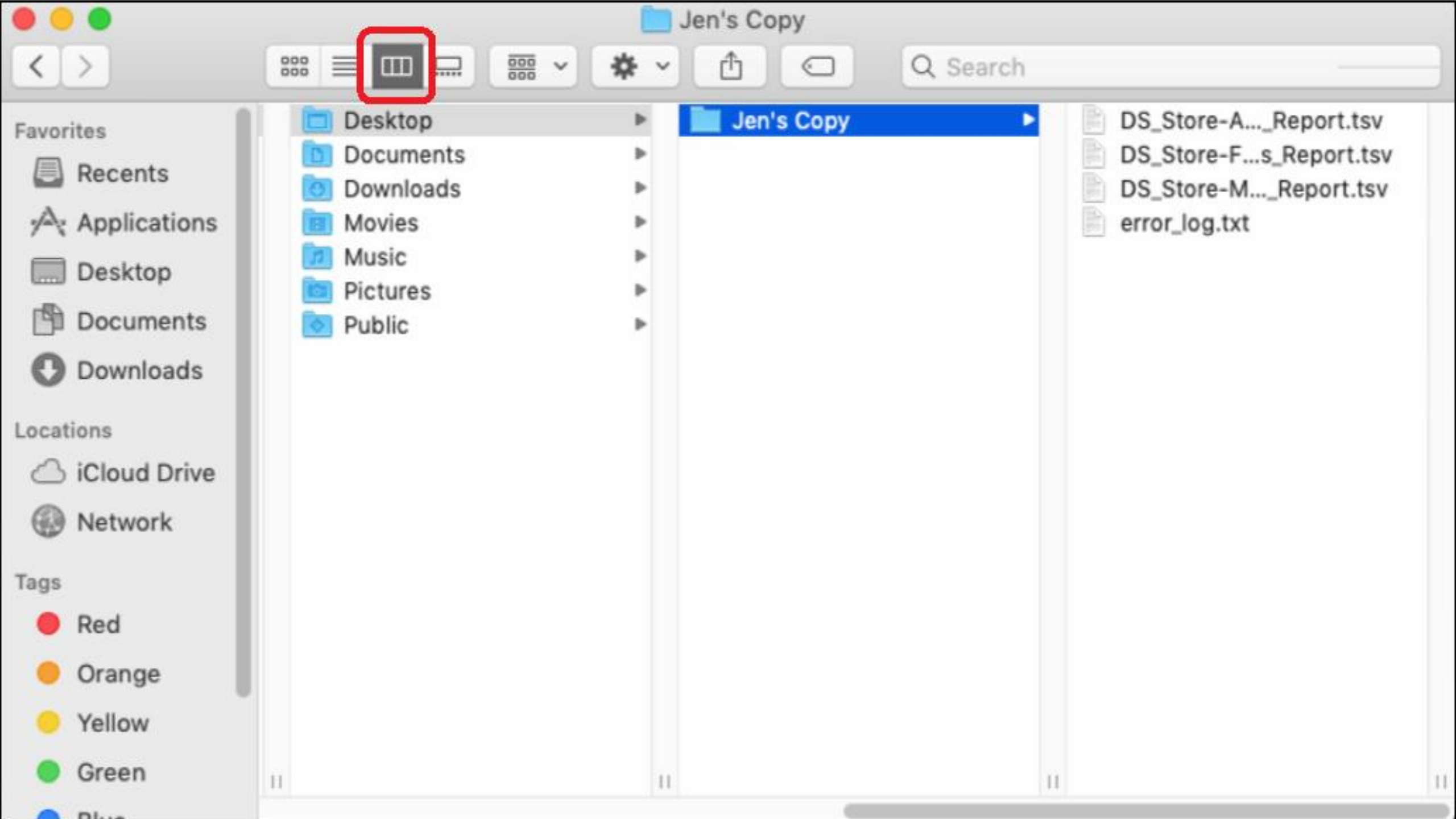
Introduction to .DS_Stores

.DS_Stores and Finder Views

.DS_Stores and Finder Views

“columns” View

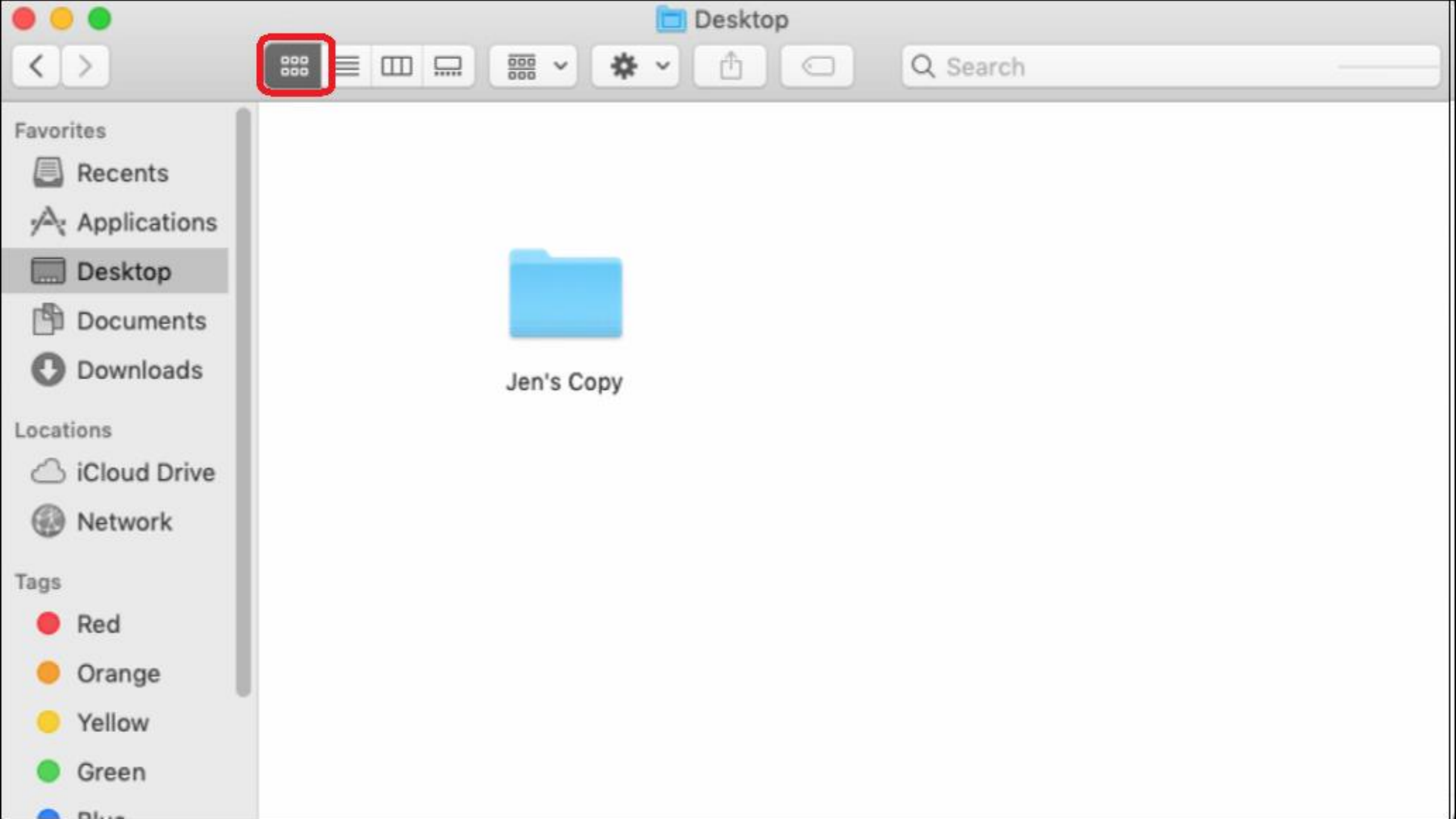
- Does NOT create/modify .DS_Stores
- A user can navigate through folders with no effect to .DS_Stores


Jen's Copy
Search
Favorites
Recents
Applications
Desktop
Documents
Downloads
Locations
iCloud Drive
Network
Tags
Red
Orange
Yellow
Green
Desktop
Documents
Downloads
Movies
Music
Pictures
Public
Jen's Copy
DS_Store-A..._Report.tsv
DS_Store-F...s_Report.tsv
DS_Store-M..._Report.tsv
error_log.txt

.DS_Stores and Finder Views

"icon" View

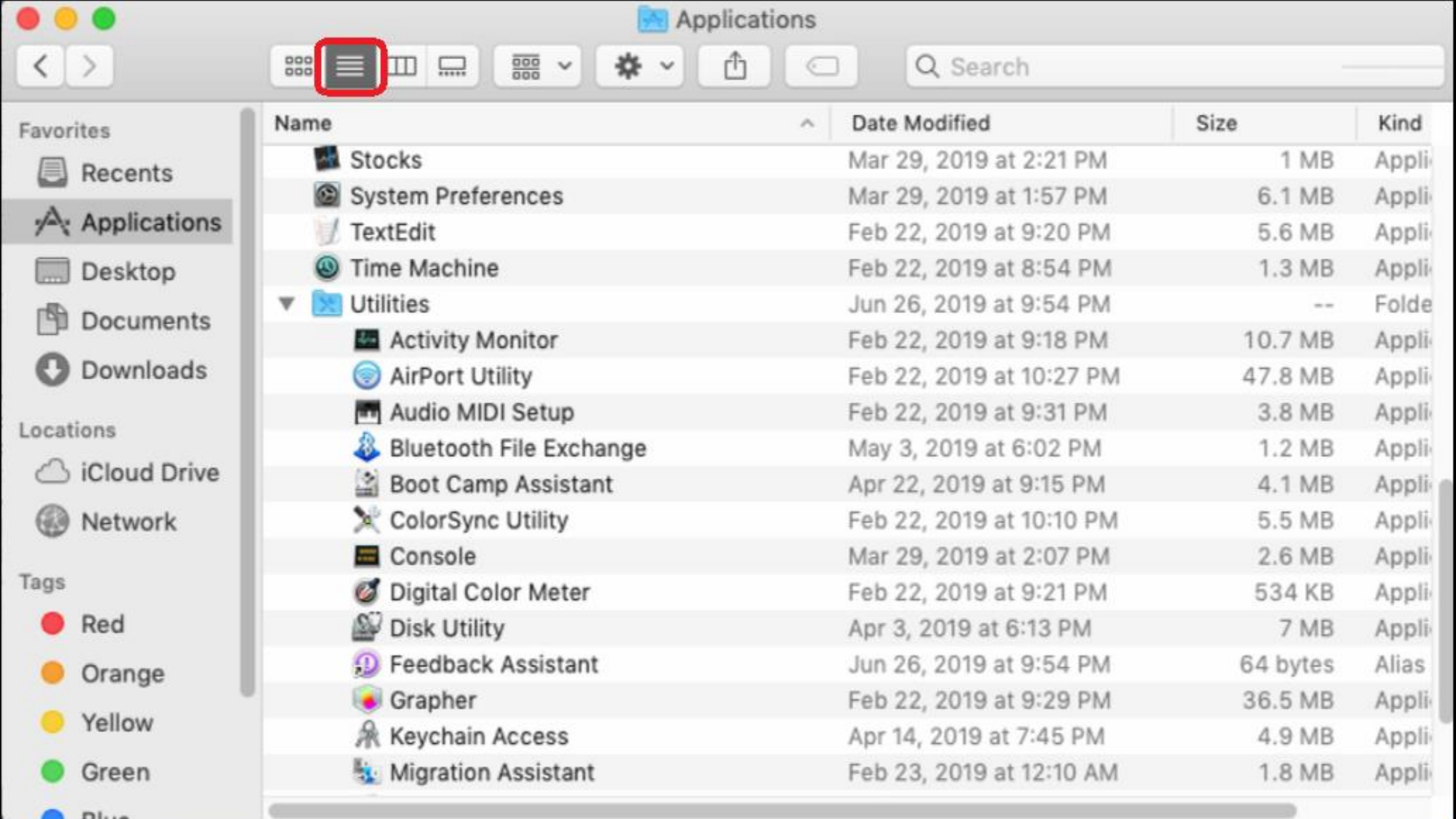
- Creates/modifies a .DS_Store
- Parent folder's .DS_Store contains
  - The view setting for the folder: Icon View
- .DS_Store of folder contains
  - Location of icons
  - Selected index of files (OS versions prior to MacOS Sierra)


Desktop
Search
Favorites
Recents
Applications
Desktop
Documents
Downloads
Locations
iCloud Drive
Network
Tags
Red
Orange
Yellow
Green
Jen's Copy

.DS_Stores and Finder Views

"list" View

- Creates/modifies a .DS_Store
- Parent folder's .DS_Store contains
  - The view setting for the folder: List View
- Folder's .DS_Store contains
  - The disclosure (dscl) status of a sub-folder
    - 0 = False, the folder is not currently disclosed (but previously was)
    - 1 = True, the folder is currently disclosed


Applications
Search
Favorites
Recents
Applications
Desktop
Documents
Downloads
Locations
iCloud Drive
Network
Tags
Red
Orange
Yellow
Green
Name
Date Modified
Size
Kind
Stocks Mar 29, 2019 at 2:21 PM 1 MB Appli
System Preferences Mar 29, 2019 at 1:57 PM 6.1 MB Appli
TextEdit Feb 22, 2019 at 9:20 PM 5.6 MB Appli
Time Machine Feb 22, 2019 at 8:54 PM 1.3 MB Appli
Utilities Jun 26, 2019 at 9:54 PM -- Folde
Activity Monitor Feb 22, 2019 at 9:18 PM 10.7 MB Appli
AirPort Utility Feb 22, 2019 at 10:27 PM 47.8 MB Appli
Audio MIDI Setup Feb 22, 2019 at 9:31 PM 3.8 MB Appli
Bluetooth File Exchange May 3, 2019 at 6:02 PM 1.2 MB Appli
Boot Camp Assistant Apr 22, 2019 at 9:15 PM 4.1 MB Appli
ColorSync Utility Feb 22, 2019 at 10:10 PM 5.5 MB Appli
Console Mar 29, 2019 at 2:07 PM 2.6 MB Appli
Digital Color Meter Feb 22, 2019 at 9:21 PM 534 KB Appli
Disk Utility Apr 3, 2019 at 6:13 PM 7 MB Appli
Feedback Assistant Jun 26, 2019 at 9:54 PM 64 bytes Alias
Grapher Feb 22, 2019 at 9:29 PM 36.5 MB Appli
Keychain Access Apr 14, 2019 at 7:45 PM 4.9 MB Appli
Migration Assistant Feb 23, 2019 at 12:10 AM 1.8 MB Appli

Parsing .DS_Stores

- Open source and free python based tool DSStoreParser:
  - https://github.com/nicoleibrahim/DSStoreParser
- Compiled builds are available here:
  - https://github.com/nicoleibrahim/DSStoreParser/releases
- Outputs three reports in tsv format:
  - DS_Store-Folder_Access_Report
  - DS_Store-Miscellaneous_Info_Report
  - DS_Store-All_Parsed_Report

Parsing .DS_Stores
DSStoreParser Usage

```
usage: DSStoreParser.py [-h] -s SOURCE -o OUTDIR [-f]

DSStoreParser CLI tool. v0.2.1

Search for .DS_Store files in the path provided and parse them.

optional arguments:
  -h, --help            show this help message and exit
  -s SOURCE, --source SOURCE
                        The source path to search recursively for .DS_Store
                        files to parse.
  -o OUTDIR, --out OUTDIR
```

Parsing .DS_Stores
DSStoreParser Reports

DS_Store-Folder_Access_Report

Record types related to folder access:

- dscl/fdsc: Directory disclosure status
- bRsV: Browse in selected view
- bwsp: Browser window properties
- icgo/icsp/ICVO/icvo/icvp/icvt: Icon view properties
- lsvC/LSVO/lsvo/lsvt/lsvP/lsvp/lssp: List view properties
- vSrn: Opened in new tab
- vstl: View style selected
- glvp: Gallery view properties
- fwi0/fwsw/fwvh/info: Finder properties
- pBB0/pBBk/pict/BKGD: Background picture settings

DS_Store-Miscellaneous_Info_Report

Other record types:

- clip: Text clipping
- cmmt: Finder comments
- dilc/Iloc: Icon locations
- extn: File extension
- lg1S/logS: Logical size
- modD/moDD: Modified date
- ph1S/phyS: Physical size
- ptbL/ptbN: Trash Put Back information

Interesting Correlations
Window Bounds

- bwsp: Browser Window Settings
- This record type contains the window bounds (location of the Finder window)
- Double-clicking on folders while in Icon view
- Provides the ability to correlate folder accesses
- As a user navigates through folders, each .DS_Store entry is updated with the current bounds.

Interesting Correlations
Window Bounds

generated_path	record_filename	record_type	record_format	record_data
/Users/Niko/Desktop/My_Images	My_Images	bwsp	blob (PlistCodec)	{'ShowStatusBar': False, 'WindowBounds': '{{433, 148}, {925, 673}}', 'ContainerShowSidebar': True, 'SidebarWidth': 192, 'ShowTabView': False, 'PreviewPaneVisibility': False, 'ShowToolbar': True, 'ShowSidebar': True, 'ShowPathbar': False}
/Users/Niko/Desktop/My_Images/2017-Images	2017-Images	bwsp	blob (PlistCodec)	{'ShowStatusBar': False, 'WindowBounds': '{{433, 148}, {925, 673}}', 'ContainerShowSidebar': True, 'SidebarWidth': 192, 'ShowTabView': False, 'PreviewPaneVisibility': False, 'ShowToolbar': True, 'ShowSidebar': True, 'ShowPathbar': False}

Interesting Correlations
Window Bounds

generated_path	record_type	record_data
/Users/neiko/Desktop/knowC/Private/Knowledge	bwsp (Browser	{'ShowStatusBar': True, 'WindowBounds': '{{230, 335}, {1145, 436}}', 'ContainerShowSidebar': True, 'ShowTabView': True, 'ShowToolbar': True, 'ShowPathbar': True, 'ShowSidebar': True}
/Users/neiko/Desktop/knowC/Private	bwsp (Browser	{'ShowStatusBar': True, 'WindowBounds': '{{230, 335}, {1145, 436}}', 'ContainerShowSidebar': True, 'ShowTabView': True, 'ShowToolbar': True, 'ShowPathbar': True, 'ShowSidebar': True}
/Users/neiko/Desktop/knowC/nikki	bwsp (Browser	{'ShowStatusBar': True, 'WindowBounds': '{{230, 335}, {1145, 436}}', 'ContainerShowSidebar': True, 'ShowTabView': True, 'ShowToolbar': True, 'ShowPathbar': True, 'ShowSidebar': True}
/Users/nikki/Development/04-KnowledgeC/26-SQLiteDB_to_TSV/parsed/20190324	bwsp (Browser	{'ShowStatusBar': True, 'WindowBounds': '{{230, 335}, {1145, 436}}', 'ContainerShowSidebar': True, 'ShowTabView': True, 'ShowToolbar': True, 'ShowPathbar': True, 'ShowSidebar': True}
/Users/nikki/Development/04-KnowledgeC/26-SQLiteDB_to_TSV/parsed	bwsp (Browser	{'ShowStatusBar': True, 'WindowBounds': '{{230, 335}, {1145, 436}}', 'ContainerShowSidebar': True, 'ShowTabView': True, 'ShowToolbar': True, 'ShowPathbar': True, 'ShowSidebar': True}
/Users/nikki/Development/04-KnowledgeC/26-SQLiteDB_to_TSV	bwsp (Browser	{'ShowStatusBar': True, 'WindowBounds': '{{230, 335}, {1145, 436}}', 'ContainerShowSidebar': True, 'ShowTabView': True, 'ShowToolbar': True, 'ShowPathbar': True, 'ShowSidebar': True}

Interesting Correlations
Scroll Positions

- icvp: Icon view properties
- lsvC: List view columns
- lsvp: List view properties
- Contains both vertical and horizontal scroll positions
- Provides insight about the last visible area the user was viewing

Interesting Correlations
Scroll Positions

generated_path	record_type	record_data
/.	lsvp (List View	{'sortColumn': 'name', 'textSize': 12.0, 'viewOptionsVersion': 1, 'calculateAllSizes': False, 'iconSize': 16.0, 'showIconPreview': True, 'scrollPositionY': 91.0, 'scrollPositionX': 0.0, 'useRelativeDates': True, 'columns': {'kind': {'index': 4, 'ascending': True, 'visible': True, 'width': 115}, 'name': {'visible': True, 'ascending': True, 'index': 0, 'width': 816}, 'dateLastOpened': {'index': 8, 'ascending': False, 'visible': False, 'width': 200}, 'comments': {'index': 7, 'ascending': True, 'visible': False, 'width': 300}, 'label': {'index': 5, 'ascending': True, 'visible': False, 'width': 100}, 'version': {'index': 6, 'ascending': True, 'visible': False, 'width': 75}, 'dateCreated': {'index': 2, 'ascending': False, 'visible': False, 'width': 181}, 'dateModified': {'index': 1, 'ascending': False, 'visible': True, 'width': 181}, 'size': {'index': 3, 'ascending': False, 'visible': True, 'width': 97}}}
/.fseventsd	lsvp (List View	{'sortColumn': 'dateModified', 'textSize': 12.0, 'viewOptionsVersion': 1, 'calculateAllSizes': False, 'iconSize': 16.0, 'showIconPreview': True, 'scrollPositionY': 0.0, 'scrollPositionX': 0.0, 'useRelativeDates': True, 'columns': {'kind': {'index': 4, 'ascending': True, 'visible': True, 'width': 115}, 'name': {'visible': True, 'ascending': True, 'index': 0, 'width': 252}, 'dateLastOpened': {'index': 8, 'ascending': False, 'visible': False, 'width': 200}, 'comments': {'index': 7, 'ascending': True, 'visible': False, 'width': 300}, 'label': {'index': 5, 'ascending': True, 'visible': False, 'width': 100}, 'version': {'index': 6, 'ascending': True, 'visible': False, 'width': 75}, 'dateCreated': {'index': 2, 'ascending': False, 'visible': False, 'width': 181}, 'dateModified': {'index': 1, 'ascending': False, 'visible': True, 'width': 181}, 'size': {'index': 3, 'ascending': False, 'visible': True, 'width': 97}}}
/Applications	lsvp (List View	{'sortColumn': 'name', 'textSize': 12.0, 'viewOptionsVersion': 1, 'calculateAllSizes': False, 'iconSize': 16.0, 'showIconPreview': True, 'scrollPositionY': 1185.0, 'scrollPositionX': 3.0, 'useRelativeDates': True, 'columns': {'kind': {'visible': True, 'ascending': True, 'index': 4, 'width': 115}, 'name': {'visible': True, 'ascending': True, 'index': 0, 'width': 356}, 'dateLastOpened': {'visible': False, 'ascending': False, 'index': 8, 'width': 200}, 'comments': {'visible': False, 'ascending': True, 'index': 7, 'width': 300}, 'label': {'visible': False, 'ascending': True, 'index': 5, 'width': 100}, 'version': {'visible': False, 'ascending': True, 'index': 6, 'width': 75}, 'dateCreated': {'visible': False, 'ascending': False, 'index': 2, 'width': 181}, 'dateModified': {'visible': True, 'ascending': False, 'index': 1, 'width': 181}, 'size': {'visible': True, 'ascending': False, 'index': 3, 'width': 97}}}

Interesting Correlations
Trash Put Backs

- ptbN: Trash Put Back Name
- ptbL: Trash Put Back Location
- Contains the original filename and location of a file/folder sent to the Trash
- Follows the file even if restored, renamed, or moved
- Provides insight about the original name/location of files that were sent to the Trash

Interesting Correlations
Trash Put Backs

generated_path	record_type	record_data
/Users/neiko/.Trash/000000000194adf1	ptbL (Trash Put Back Location)	Users/neiko/Desktop/
/Users/neiko/.Trash/000000000194adf1	ptbN (Trash Put Back Name)	000000000194adf1
/Users/neiko/.Trash/osxpmem.app	ptbL (Trash Put Back Location)	/
/Users/neiko/.Trash/osxpmem.app	ptbN (Trash Put Back Name)	osxpmem.app
/Users/neiko/Desktop/DS_Store/ds_store-bash.ad1.txt	ptbL (Trash Put Back Location)	Users/neiko/Desktop/DS_Store/
/Users/neiko/Desktop/DS_Store/ds_store-bash.ad1.txt	ptbN (Trash Put Back Name)	ds_store-bash.ad1.txt
/Users/neiko/Desktop/New folder/knowC_rename_test	ptbL (Trash Put Back Location)	Users/neiko/Desktop/KnowledgeC/
/Users/neiko/Desktop/New folder/knowC_rename_test	ptbN (Trash Put Back Name)	knowC
/Users/other/Desktop/Script.sh	ptbL (Trash Put Back Location)	Users/lilly/Desktop/
/Users/other/Desktop/Script.sh	ptbN (Trash Put Back Name)	Script.sh

Interesting Correlations
Selected Indexes

- Iloc: Icon location
- Contains an index number if a file or folder was selected
- Provides insight into files/folders the user selected/clicked on
- Unfortunately, deprecated as of MacOS 10.12 Sierra

Interesting Correlations
Selected Indexes

generated_path	record_type	record_data
/Users/nikki/Development/.DS_Store	Iloc (Icon Location)	Location: (472, 40), Selected Index: 9, Unknown: ffff0000
/Users/nikki/Development/ds_store_parser.py	Iloc (Icon Location)	Location: (204, 264), Selected Index: 26, Unknown: ffff0000
/Users/nikki/Development/FSEventWatcher	Iloc (Icon Location)	Location: (338, 40), Selected Index: 2, Unknown: ffff0000
/Users/nikki/Development/FSEventWatcher.zip	Iloc (Icon Location)	Location: (204, 40), Selected Index: 1, Unknown: ffff0000
/Users/nikki/Development/logs	Iloc (Icon Location)	Location: (338, 264), Selected Index: 20, Unknown: ffff0000
/Users/nikki/Development/logs.dmg	Iloc (Icon Location)	Location: (70, 376), Selected Index: Null, Unknown: ffff0000
/Users/nikki/Development/M1-Test-Shared_Folder_Desktop	Iloc (Icon Location)	Location: (275, 159), Selected Index: 21, Unknown: ffff0000
/Users/nikki/Development/original.txt	Iloc (Icon Location)	Location: (204, 488), Selected Index: Null, Unknown: ffff0000
/Users/nikki/Development/Parallels Shared Folders	Iloc (Icon Location)	Location: (70, 40), Selected Index: Null, Unknown: ffff0000
/Users/nikki/Development/test.txt	Iloc (Icon Location)	Location: (338, 488), Selected Index: 25, Unknown: ffff0000
/Users/nikki/Development/Tests_output	Iloc (Icon Location)	Location: (70, 264), Selected Index: 27, Unknown: ffff0000
/Users/nikki/Development/untitled folder	Iloc (Icon Location)	Location: (472, 264), Selected Index: 24, Unknown: ffff0000

Caveats

- .DS_Stores are portable
- No full paths
- No stored timestamps
- Data is volatile

Caveats
.DS_Stores are Portable

Problem:

- .DS_Stores can be archived in a container file such as a ZIP, then unzipped on another computer.
- Copying folders also copies hidden .DS_stores

Solution:

- This solution does not apply to files parsed on Windows systems
- Check permissions
  - Expected: -rw-r--r--
  - Only the owner has r/w access by default
  - The three files that exist by default on a fresh install are an exception
- Check extended attributes
  - Expected: “com.apple.finderinfo”

Caveats
No Full Paths

Problem:

- Full paths are not stored in .DS_Stores

Solution:

- The DSStoreParser tool builds the full path using the path to the .DS_Store file

Caveats
No Stored Timestamps

Problem:

- There are no stored timestamps that indicate when a record was added or changed

Solution:

- None
- The created/modified timestamps of the .DS_Store file provides a time range at best

Caveats
Record Data is Volatile

Problem:

- .DS_Stores do not retain previous records
- When an item is deleted or moved all associated records are purged
- When items are renamed all associated records are updated with the new name

Solution:

- Carving for .DS_Store files
- Check local snapshots
- Check Time Machine backups

Conclusion

- .DS_Stores are created as a result of user interaction
- They provide evidence of folder accesses
- They provide insight into how the user interacted with files/folders
- Original file names and locations can be identified using Trash Put Backs
- Some caveats, can be overcome

Questions?

Nicole Ibrahim | Senior Associate, Cyber Response | KMPG, LLP

nicoleibrahim@kpmg.com | @nicoleibrahim