

# CSC469: Assignment 1

Rohan Chandra

Oct/3/2011

996274142

chandr39

1a)

Using TSK: autopsy, under the image details page, the following information was uncovered:

### Image details:

The investigation revealed that the source operating system is linux, that file system type is Ext2, and the volume is unnamed, but has ID df0fe07088a85dae2f41dfc4e6fd7e65 . The File system was last accessed on Friday February 13 2004 at 00:25:10 , was last checked on Sunday February 8 2004 at 19:03:19, and was last mounted at Friday February 2004 at 13 00:20:54 .

Analysis revealed that drive has an inode range of 1 to 185, with 165 free inodes and the block range runs from 0 – 1439, with a block size 1024 and 501 free blocks. The root directory begins at block 2 and block 1 is reserved. The image contains 1 block groups containing 184 inodes and 8192 blocks. This group, group 0, contains the inodes in range 1-184 and the blocks in range 1 – 1439.

The layout of block group 0 was discovered as follows. The super block was found to occur at block 1, the group descriptor table at block 2, the data bitmap at block 3, the inode bitmap at block 4, the inode table in blocks 5-27, and the data blocks in blocks 28-1439. Finally, the block group contains 3 directories, has 165 free inodes and 501 (34%) free blocks.

The three directories are as follows:

### Root directory details:


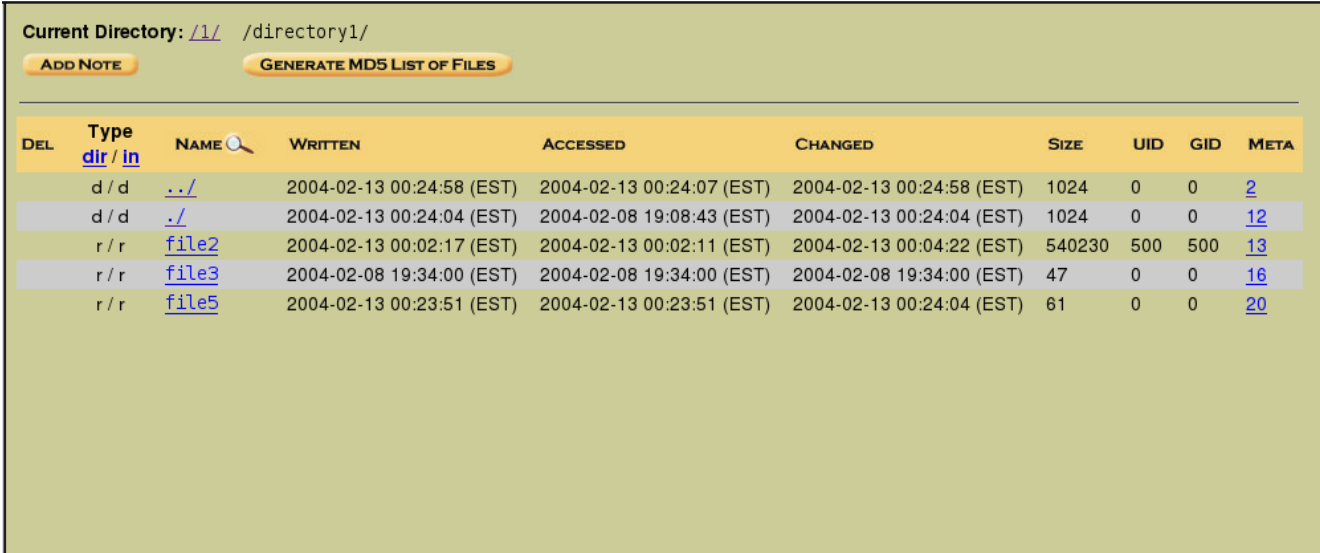
Current Directory: <a href="#">/1/</a>									
<a href="#">ADD NOTE</a>		<a href="#">GENERATE MD5 LIST OF FILES</a>							
DEL	Type <a href="#">dir / in</a>	NAME 	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	d / d	<a href="#">\$OrphanFiles/</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<a href="#">185</a>
	d / d	<a href="#">../</a>	2004-02-13 00:24:58 (EST)	2004-02-13 00:24:07 (EST)	2004-02-13 00:24:58 (EST)	1024	0	0	<a href="#">2</a>
	d / d	<a href="#">./</a>	2004-02-13 00:24:58 (EST)	2004-02-13 00:24:07 (EST)	2004-02-13 00:24:58 (EST)	1024	0	0	<a href="#">2</a>
✓	r / -	<a href="#">.file3.swp</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	0
✓	r / -	<a href="#">.file3.swpx</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	0
	r / r	<a href="#">DCP_1722.JPG</a>	2001-10-19 01:15:32 (EDT)	2004-02-13 00:00:00 (EST)	2004-02-13 00:11:34 (EST)	315647	500	500	<a href="#">19</a>
	d / d	<a href="#">directory1/</a>	2004-02-13 00:24:04 (EST)	2004-02-08 19:08:43 (EST)	2004-02-13 00:24:04 (EST)	1024	0	0	<a href="#">12</a>
✓	r / -	<a href="#">file2</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	0
	r / r	<a href="#">file3</a>	2004-02-13 00:23:13 (EST)	2004-02-13 00:23:13 (EST)	2004-02-13 00:23:13 (EST)	61	0	0	<a href="#">21</a>
	r / r	<a href="#">file4</a>	2004-02-08 19:36:25 (EST)	2004-02-08 19:36:25 (EST)	2004-02-08 19:36:25 (EST)	47	0	0	<a href="#">17</a>
✓	r / -	<a href="#">handle.pdf</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	0
	r / r	<a href="#">index.dat</a>	2004-02-08 15:12:48 (EST)	2004-02-10 00:00:00 (EST)	2004-02-13 00:06:22 (EST)	49152	500	500	<a href="#">14</a>
	d / d	<a href="#">lost+found/</a>	2004-02-08 19:03:21 (EST)	2004-02-08 19:03:21 (EST)	2004-02-08 19:03:21 (EST)	12288	0	0	<a href="#">11</a>

figure 1: the files under the root directory.

The root directory contained the following files in figure 1. The pdf seen in figure 1, likely corresponds to the file “OrphanFile-18”, which can be exported and revealed to be a pdf on digital forensics, Eoghan-ch23.qxd 1/5/04 4:56 PM Page 625-632. Additionally files, “file3” and “file4” are text files that contain strings that indicate the date on which they were created. Finally, the file “index.dat” contains a listing of url's of images viewed by the user on a local network. It is possible that this file is the “index.dat” file created by a web browser program, specifically internet explorer, as a caching mechanism to improve browser performance, as is indicated on the forensics open source wiki (see work cited below). The header of the index.dat file (image appears at appendix, section 1, part b) begins as "Client UrlCache MMF Ver 5.2", which is the same as the header used by all internet explorer files since internet explorer 5. Finally, the image DCP\_1722 is a picture of what appears to be a hard disk.

## Directory 1:



Current Directory: [/1/](#) /directory1/

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)


DEL	Type <a href="#">dir</a> / <a href="#">in</a>	NAME 	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	d / d	<a href="#">../</a>	2004-02-13 00:24:58 (EST)	2004-02-13 00:24:07 (EST)	2004-02-13 00:24:58 (EST)	1024	0	0	<a href="#">2</a>
	d / d	<a href="#">./</a>	2004-02-13 00:24:04 (EST)	2004-02-08 19:08:43 (EST)	2004-02-13 00:24:04 (EST)	1024	0	0	<a href="#">12</a>
	r / r	<a href="#">file2</a>	2004-02-13 00:02:17 (EST)	2004-02-13 00:02:11 (EST)	2004-02-13 00:04:22 (EST)	540230	500	500	<a href="#">13</a>
	r / r	<a href="#">file3</a>	2004-02-08 19:34:00 (EST)	2004-02-08 19:34:00 (EST)	2004-02-08 19:34:00 (EST)	47	0	0	<a href="#">16</a>
	r / r	<a href="#">file5</a>	2004-02-13 00:23:51 (EST)	2004-02-13 00:23:51 (EST)	2004-02-13 00:24:04 (EST)	61	0	0	<a href="#">20</a>

figure 2: a screen shot of directory1, a directory under the root directory.

Directory1 contained an image of a cityscape in the file “file2”. Files “file3” and “file5” that contain strings indicating the times at which they were created. The file, “file3” does not appear to correspond to the “file3” in the root directory. The file “file2” may be a copy of the “file2” that was deleted in the root directory, but further investigation was not performed to confirm this.

## Orphan files:

Current Directory: [/1/](#) /\$OrphanFiles/

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	<a href="#">dir</a> / <a href="#">in</a>								
✓	- / r	<a href="#">OrphanFile-15</a>	2004-02-08 19:10:46 (EST)	2004-02-08 19:10:46 (EST)	2004-02-13 00:24:21 (EST)	47	0	0	<a href="#">15</a>
✓	- / r	<a href="#">OrphanFile-18</a>	2004-02-13 00:07:49 (EST)	2004-02-13 00:07:49 (EST)	2004-02-13 00:24:58 (EST)	80117	500	500	<a href="#">18</a>

Figure 3: the orphan files in image 1

The OrphanFile-15 is a text file that contains a string that indicates the time at which it was created, it is possible that this file corresponds to the deleted file “file2” in the root directory, but further investigation into this was not explored. OrphanFile-18 likely corresponds to handle.pdf in the root directory as discussed previously.

**b)**

**Additional analysis of image 1 using FTK.**

Follow up analysis using FTK confirmed initial finding discovered using autopsy of the images details and no new information was noted about the image details, or the directory structures. The confirmation of the image layout and details can be seen in appendix section 2, part b. However, the analysis in FTK did not show the following files, “.file3.swp”, “.file3.swpx”, or “handle.pdf”.

However, it was noted that the image files found previously were not taken with the same model camera. This fact was discovered by examining the htm files associated with each image. Furthermore, it was confirmed that the index.dat (image located at appendix section 2, part a) was created by some version of Microsoft internet explorer, though FTK likely determined using the same file header information as lead to the same conclusion in part a. As shown in appendix section b part 1, FTK indicated additional information about the access times of these local files and indicated the user name as “eco”, which correlates with original findings in the autopsy analysis of the index.dat file.

C)

### Analysis of image 2 using Autopsy:

Using Autopsy's image details page, the following information was procured:

The image is using the Ext3 filesystem and the volume is named KW\_Ssearch with ID a68756a9e8db74bd7f424a02197130e2 .The file system was last written to on Sunday, November, 23, 2003 at 2:06 pm, was last checked on Sunday, November, 23, 2003 at 1:54 pm and was last pointed on Sunday, November, 23, 2003 at 2:04 pm. The operating system used on the file system was Linux and the journal is located at inode 8.

Subsequent analysis reveled that drive has an inode range of 1 to 1281, with 1266 free inodes and the block range runs from 0 – 5119, with a block size 1024 and 3908 free blocks. The root directory begins at block 2 and block 1 is reserved. The File system contains 1 block groups containing 1280 inodes and 8192 blocks. Group 0, contains the inodes in range 1-184 and the blocks in range 1 – 1439.

In examining the layout of block group 0, the super block was found to occur at block 1, the group descriptor table at block 2, the data bitmap at block 3, the inode bitmap at block 4, the inode table in blocks 5-164, and the data blocks in blocks 165-5119. Finally, the block group contains 1 directory, has 1266 free inodes and 3908 (76%) free blocks.

Root directory:

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	d / d	<a href="#">\$OrphanFiles/</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<a href="#">1281</a>
	d / d	<a href="#">../</a>	2003-11-23 15:06:28 (EST)	2003-11-23 15:06:21 (EST)	2003-11-23 15:06:28 (EST)	1024	500	500	<a href="#">2</a>
	d / d	<a href="#">./</a>	2003-11-23 15:06:28 (EST)	2003-11-23 15:06:21 (EST)	2003-11-23 15:06:28 (EST)	1024	500	500	<a href="#">2</a>
	r / r	<a href="#">file1</a>	2003-11-23 15:03:54 (EST)	2003-11-23 15:03:54 (EST)	2003-11-23 15:03:54 (EST)	601	0	0	<a href="#">12</a>
	r / r	<a href="#">file2</a>	2003-11-23 15:06:03 (EST)	2003-11-23 15:04:06 (EST)	2003-11-23 15:06:03 (EST)	1300	0	0	<a href="#">13</a>
✓	r / r	<a href="#">file3</a>	2003-11-23 15:06:28 (EST)	2003-11-23 15:04:23 (EST)	2003-11-23 15:06:28 (EST)	0	0	0	<a href="#">14</a>
	r / r	<a href="#">first</a>	2003-11-23 15:04:36 (EST)	2003-11-23 15:04:36 (EST)	2003-11-23 15:04:36 (EST)	63	0	0	<a href="#">15</a>
	d / d	<a href="#">lost+found/</a>	2003-11-23 14:54:16 (EST)	2003-11-23 14:54:16 (EST)	2003-11-23 14:54:16 (EST)	12288	0	0	<a href="#">11</a>

Figure 1: the root directory of the image

Analysis of the root directory discovered little of note. There were no orphan files and no further information could be found about the deleted file, “file 3”. Files “file1” and “file2” contain the words first and second respectively and what appears to be corrupt text or non-human readable text elsewhere, though the files may be internal data files. The File “first” appears to be empty, but checking the hex of the file reveals some random non human readable text.

**d)**

**Analysis of image 2 using FTK**

Analysis using FTK revealed no additional information about the file system structure (image of structure at appendix, section 4, part a). However, it was noted that FTK indicated the file type of the block and inode bitmaps and associated structures were Ext2 metadata file types. However, since I did not have an additional Ext3 image to compare against, I was unable to conclude if this was an irregularity in the image, or if this is the expected behavior of ftk.

## **Question 1 APPENDIX:**

### **Work cited and external resources used:**

[http://www.forensicswiki.org/wiki/Internet\\_Explorer\\_History\\_File\\_Format](http://www.forensicswiki.org/wiki/Internet_Explorer_History_File_Format) – for information on index.dat found in root directory of image 1.

### **Section 1a)**

#### **Autopsy image 1 details output:**

#### **FILE SYSTEM INFORMATION**

File System Type: Ext2

Volume Name:

Volume ID: df0fe07088a85dae2f41dfc4e6fd7e65

Last Written at: Fri Feb 13 00:25:10 2004

Last Checked at: Sun Feb 8 19:03:19 2004

Last Mounted at: Fri Feb 13 00:20:54 2004

Unmounted properly

Last mounted on:

Source OS: Linux

Dynamic Structure

InCompat Features: Filetype,

Read Only Compat Features: Sparse Super,

#### **METADATA INFORMATION**

Inode Range: 1 - 185

Root Directory: 2

Free Inodes: 165

#### **CONTENT INFORMATION**

Block Range: 0 - 1439

Block Size: 1024

Reserved Blocks Before Block Groups: 1

Free Blocks: 501

#### **BLOCK GROUP INFORMATION**

Number of Block Groups: 1

Inodes per group: 184

Blocks per group: 8192

Group: 0:

Inode Range: 1 - 184

Block Range: 1 - 1439

Layout:

Super Block: 1 - 1

Group Descriptor Table: 2 - 2

Data bitmap: 3 - 3

Inode bitmap: 4 - 4

Inode Table: 5 - 27

Data Blocks: 28 - 1439

Free Inodes: 165 (16500%)



Free Blocks: 501 (34%)  
Total Directories: 3

**Analysis of root directory:**

**Pointed to by file:**

/1/

/1/ .

/1/ ..

/1/lost+found/..

/1/directory1/..

**File Type:**

data

**MD5 of content:**

cc4fd1b1668d7f710977e34974079122 -

**SHA-1 of content:**

e13ec2896ee871ee45cb56012bfb5eb03b5a888a -

**Details:**

inode: 2

Allocated

Group: 0

Generation Id: 0

uid / gid: 0 / 0

mode: drwxr-xr-x

size: 1024

num of links: 4

**Inode Times:**

Accessed: Fri Feb 13 00:24:07 2004

File Modified: Fri Feb 13 00:24:58 2004

Inode Modified: Fri Feb 13 00:24:58 2004

Direct Blocks:

[28](#)

Section 1 part b)  
Contents of the file: index.dat in the root directory of image :

Client UrlCache MMF Ver 5.2  
HASH  
URL  
Visited: eco@http://192.168.0.5:8080  
URL  
Visited: eco@http://192.168.0.5:8080/IMG009.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG001.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG002.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG003.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG004.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG005.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG006.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG007.JPG  
URL  
Visited: eco@http://192.168.0.5:8080/IMG008.JPG  
URL

Section 2:  
part a) partial analysis of index.dat

index.dat
Internet Explorer Master Browsing History
URL http://192.168.0.5:8080/IMG000.JPG
User name eco
Page title
Last Accessed (UTC) 2/8/2004 8:03:46 PM
Last Accessed-2 (UTC) 2/8/2004 8:03:46 PM
Last Checked (UTC) 2/8/2004 8:03:48 PM

part b)The files in the image found using FTK

15	a1-image1\N\NAME-ext2\{orphan}\15	Unknown File Type	Unknown	2/13/2004 12:24:21 ...	2/8/2004 7:10:46 PM	2/8/2004 7:10:46 PM
18	a1-image1\N\NAME-ext2\{orphan}\18	Acrobat Portable Document F...	Document	2/13/2004 12:24:58 ...	2/13/2004 12:07:49 ...	2/13/2004 12:07:49 ...
[Root Folder]	a1-image1\N\NAME-ext2	Root Folder	Folder	2/13/2004 12:24:58 ...	2/13/2004 12:24:58 ...	2/13/2004 12:24:07 ...
Bad Blocks	a1-image1\N\NAME-ext2\Bad Blocks	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A
Block Bitmap	a1-image1\N\NAME-ext2\Block Bitmap	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A
Boot Record	a1-image1\N\NAME-ext2\Boot Record	Volume Boot Record	Slack/Free S...	N/A	N/A	N/A
DCP_1722.JPG	a1-image1\N\NAME-ext2\DCP_1722.JPG	JPEG/Exif file	Graphic	2/13/2004 12:11:34 ...	10/19/2001 1:15:32 ...	2/13/2004 12:00:00 ...
DCP_1722.JPG.htm	a1-image1\N\NAME-ext2\DCP_1722.JPG>>DC...	htm	Hypertext Document	N/A	N/A	N/A
directory1	a1-image1\N\NAME-ext2\directory1	Folder	Folder	2/13/2004 12:24:04 ...	2/13/2004 12:24:04 ...	2/8/2004 7:08:43 PM
DriveFreeSpace1	a1-image1\N\NAME-ext2\DriveFreeSpace1	Drive Free Space	Slack/Free S...	N/A	N/A	N/A
file2	a1-image1\N\NAME-ext2\directory1\file2	JPEG/Exif file	Graphic	2/13/2004 12:04:22 ...	2/13/2004 12:02:17 ...	2/13/2004 12:02:11 ...
file2.htm	a1-image1\N\NAME-ext2\directory1\file2>>file2...	htm	Hypertext Document	N/A	N/A	N/A
file3	a1-image1\N\NAME-ext2\directory1\file3	Unknown File Type	Unknown	2/8/2004 7:34:00 PM	2/8/2004 7:34:00 PM	2/8/2004 7:34:00 PM
file3	a1-image1\N\NAME-ext2\file3	Unknown File Type	Unknown	2/13/2004 12:23:13 ...	2/13/2004 12:23:13 ...	2/13/2004 12:23:13 ...
file4	a1-image1\N\NAME-ext2\file4	Unknown File Type	Unknown	2/8/2004 7:36:25 PM	2/8/2004 7:36:25 PM	2/8/2004 7:36:25 PM
file5	a1-image1\N\NAME-ext2\directory1\file5	Unknown File Type	Unknown	2/13/2004 12:24:04 ...	2/13/2004 12:23:51 ...	2/13/2004 12:23:51 ...
Group Descriptor Tables	a1-image1\N\NAME-ext2\Group Descriptor Tabl...	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A
index.dat	a1-image1\N\NAME-ext2\index.dat	dat	MSIE History File	2/13/2004 12:06:22 ...	2/8/2004 3:12:48 PM	2/10/2004 12:00:00 ...
Inode Bitmap	a1-image1\N\NAME-ext2\Inode Bitmap	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A
Inode Table	a1-image1\N\NAME-ext2\Inode Table	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A
lost+found	a1-image1\N\NAME-ext2\lost+found	Folder	Folder	2/8/2004 7:03:21 PM	2/8/2004 7:03:21 PM	2/8/2004 7:03:21 PM
Superblocks	a1-image1\N\NAME-ext2\Superblocks	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A

Section 3:  
part a)  
General File System Details

FILE SYSTEM INFORMATION

File System Type: Ext3  
Volume Name: KW\_SEARCH  
Volume ID: a68756a9e8db74bd7f424a02197130e2

Last Written at: Sun Nov 23 15:06:32 2003  
Last Checked at: Sun Nov 23 14:54:16 2003

Last Mounted at: Sun Nov 23 15:04:55 2003  
Unmounted properly  
Last mounted on:

Source OS: Linux  
Dynamic Structure  
Compat Features: Journal,  
InCompat Features: Filetype,  
Read Only Compat Features: Sparse Super,

Journal ID: 00  
Journal Inode: 8

#### METADATA INFORMATION

Inode Range: 1 - 1281  
Root Directory: 2  
Free Inodes: 1266

#### CONTENT INFORMATION















Block Range: 0 - 5119  
Block Size: 1024  
Reserved Blocks Before Block Groups: 1  
Free Blocks: 3908

#### BLOCK GROUP INFORMATION

Number of Block Groups: 1  
Inodes per group: 1280  
Blocks per group: 8192

Group: 0:  
Inode Range: 1 - 1280  
Block Range: 1 - 5119  
Layout:  
Super Block: 1 - 1  
Group Descriptor Table: 2 - 2  
Data bitmap: 3 - 3  
Inode bitmap: 4 - 4  
Inode Table: 5 - 164  
Data Blocks: 165 - 5119  
Free Inodes: 1266 (126600%)  
Free Blocks: 3908 (76%)  
Total Directories: 2

Section 4:  
part a)

	[Root Folder]	a1-image2KVW_SEARCH-ext3	Root Folder	Folder	11/23/2003 3:06:28 ...	11/23/2003 3:06:28 ...	11/23/2003 3:06:21 ...	1,024	1,024	12	13
	Bad Blocks	a1-image2KVW_SEARCH-ext3Bad Blocks	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A	0	0	0	0
	Block Bitmap	a1-image2KVW_SEARCH-ext3Block Bitmap	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A	1,024	1,024	0	0
	Boot Record	a1-image2KVW_SEARCH-ext3Boot Record	Volume Boot Record	Slack/Free S...	N/A	N/A	N/A	1,024	1,024	0	0
	DriveFreeSpace1	a1-image2KVW_SEARCH-ext3DriveFreeSpace1	Drive Free Space	Slack/Free S...	N/A	N/A	N/A	4,001,792	26,214,400	0	0
	file1	a1-image2KVW_SEARCH-ext3file1	Unknown File Type	Unknown	11/23/2003 3:03:54 ...	11/23/2003 3:03:54 ...	11/23/2003 3:03:54 ...	601	1,024	0	0
	file2	a1-image2KVW_SEARCH-ext3file2	Unknown File Type	Unknown	11/23/2003 3:06:03 ...	11/23/2003 3:06:03 ...	11/23/2003 3:04:06 ...	1,300	2,048	0	0
	FileSlack	a1-image2KVW_SEARCH-ext3file1>>FileSlack	File Slack	Slack/Free S...	N/A	N/A	N/A	423	1,024	0	0
	first	a1-image2KVW_SEARCH-ext3first	Unknown File Type	Unknown	11/23/2003 3:04:36 ...	11/23/2003 3:04:36 ...	11/23/2003 3:04:36 ...	63	1,024	0	0
	Group Descriptor Tables	a1-image2KVW_SEARCH-ext3Group Descriptor ...	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A	1,024	1,024	0	0
	Inode Bitmap	a1-image2KVW_SEARCH-ext3Inode Bitmap	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A	1,024	1,024	0	0
	Inode Table	a1-image2KVW_SEARCH-ext3Inode Table	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A	163,840	163,840	0	0
	lost+found	a1-image2KVW_SEARCH-ext3lost+found	Folder	Folder	11/23/2003 2:54:16 ...	11/23/2003 2:54:16 ...	11/23/2003 2:54:16 ...	12,288	12,288	0	0
	Superblocks	a1-image2KVW_SEARCH-ext3Superblocks	Ext2 metadata	Slack/Free S...	N/A	N/A	N/A	1,024	1,024	0	0

**PART 2:**

The following actions were performed on the grey wolf temp directory. As explained on the bulletin boards, analysis revealed the home directory on greywolf is nfs and the temp directory is EXT3. Additional information about the commands performed and the exact mac time updates (or lack there of) can be followed in the adjoining appendix). Information on why I did not analyze deletion times, and my attempts to do so before reaching this decision appear after the table.

<i>Action vs MAC time category changed</i>	<b>Modified</b>	<b>Access time</b>	<b>Changed</b>
<b>Stat(file or directory)</b>	N	N	N
<b>LS (Directory)</b>	N	<b>Y</b> (listing the directory contents requires the system to read the data blocks of the directory)	N
<b>LS(file)</b>	N	N	N
<b>Echo(into a file)</b>	<b>Y</b>	N (this is likely due to the fact that echo is appending to end of the file and append may circumvent accessing the file I.e file handle opened with w only context)	<b>Y</b>
<b>Touch(directory perspective)</b>	<b>Y</b>	N (likely didn't change as it only wrote to the data blocks rather than accessing them with w/r discretionary access as was the case with appending to a file)	<b>Y</b>
<b>Creating a directory in a directory (parent directory perspective)</b> [mkdir]	<b>Y</b>	N (note performing ls in the parent directory creates an anomaly in test data)	<b>Y</b>
<b>Chmod(file or directory)</b>	N	N	<b>Y</b> (sensible as permissions are a metadata element)
<b>Chmod(files in directory whose permission changed)</b>	N	N	N (The parents permissions changed, not the children)
<b>Cat(file)</b>	N	<b>Y</b>	N
<b>CP of file (source directory)</b>	N	<b>Y</b>	N
<b>CP of file (destination directory)</b>	<b>Y</b>	N	<b>Y</b>
<b>CP(source file)</b>	N	<b>Y</b>	N
<b>CP(destination file with overwrite accepted)</b>	<b>Y</b>	N (Likely because the file is just overwritten and the writer doesn't ask for reading discretionary access, specifically point at new set of data blocks instead of reading and modifying existing ones)	<b>Y</b>
<b>CP(source file with overwrite accepted)</b>	N	<b>Y</b>	N

CP(all parties with overwrite denied)	N	N	N
Failed operation on file due to chmod	N	N	N
WC(file)	N	Y	N
Creating a file in a subdirectory (from the top level directory perspective)	N	N	N
SubDirectory removal, operation succeed (from parent directory perspective)	Y	N	Y
SubDirectory removal, operation failed (from parent directory perspective)	N	N	N
Deleting a file within a directory (Directory that contains the file perspective)	Y	N	Y
Deleting a file within a directory (Parent of the directory that contains the file perspective)	N	N	N
Hard link(file being linked to perspective)	N	N	Y
File Hard link linked to deleted (hard link perspective)	N	N	Y
File Hard link linked to Updated (hard link perspective)	N	Y	Y
Soft link(file being linked to perspective)	N	N(view stat on soft link notes for further explanation of soft link analysis)	N
File Soft link linked to updated ( Soft link perspective):	N	N	N
File Soft link linked to deleted ( Soft link perspective):	N	N	N
Stat on softlink	N	Y (Unexpected, but examining the man page of stat reveals that stat collects information about the file that the symbolic link points to, rather than the symbolic link itself, so its possible that it follows the symbolic link to the file to check its meta data triggering an access event.)	N

**Issues with examining deletion:**

The methods outlined in the carrier paper (as seen referenced in lecture), attempted to examine deletion time using either the inodes of the file or the journal of the system. Unfortunately, as students we do not have permission to directly access the inodes of a file, though we can view them using `ls -li`. Furthermore, the journal could not be accessed directly due to permissions issues, note that invoking `sudo` on a cdf machine logs an incident report with the cdf admin. Finally, I could not figure out a way to create an image of the running system such that I could analyze it using `debugfs`.

**Attempts to make deletion work in small scale controlled environment:**

As I was not able to access the inodes of the file directly or the journal of the system due to permission restriction, the following is the action I instead tried to attempt to simulate deletion within a small newly made file system under my control.

Since everything in unix is a file, I attempted to create a virtual file system using a file under my control on my own unix machine. The idea being if I could create this virtual system, I was curious if I could manipulate `pmount` such that I could mount this virtual file system and have full permissions over it. The command `mkfs`, creates a virtual file system using a give file. The command is meant to work on an existing partition, but since I cannot create partitions on CDF, I instead just created a file of large enough size, such that it was larger than a single inode, as is required by `mkfs`. To achieve this, I simply copied the contents of `/dev/random` into a file. I then used this file to act as a partition that was overwritten with the filesystem information by `mkfs`. On my own machine I was able to use `sudo` to forcibly loop mount the virtual filesystem and was able to navigate to it, create and delete files, unmount the disk and then examine the image of the disk using `debugfs` as described in the carrier paper.

Unfortunately, on cdf, I do not have permission to mount the virtual filesystem and instead attempted to use `pmount` and `gnome-mount`. However, to my knowledge and experimentation, `pmount` does not allow for loop mounting and I could not recreate the steps taken on my home machine. I did not have time to further explore how to use `gnome-mount` properly.

Additionally, I attempted to create a file, open a program (`gedit`) that then opened that file and left the program open. I deleted the file but left the program such that it would still have an open file handle to the deleted file. I examined the `proc` folder of the process id associated with the program that had the file open, then examined its open file handles to find the symbolic link to the deleted file, but could not figure out how to access deletion times from there.

Steps to recreate my experiment

```
cat /dev/random > disk &
sleep 20;
killall cat;
mkfs.ext3 disk;
mkdir diskmount;
sudo mount -o loop disk diskmount;
cd diskmount; touch file1 file2;
rm file1;
sudo umount diskmount;
debugfs disk;
```

## Question 2: APPENDIX

**CODE OUTPUT (I.e the trimmed output of the code and steps I took to created each part of the experiment):**

**Note (at some points I record creation times if they changed to search for a pattern, but did not include this in the table above as it was not necessary for the assignment)**

**Pre: LS within directory( files unaffected)**

```
greywolf:/tmp/CSC469A1$ stat top
```

File: `top'

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 809h/2057d Inode: 136274 Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandrr) Gid: ( 1009/gstudent)

Access: 2011-10-02 18:03:34.000000000 -0400

Modify: 2011-10-02 18:03:37.000000000 -0400

Change: 2011-10-02 18:03:37.000000000 -0400

```
greywolf:/tmp/CSC469A1$ cd top
```

```
greywolf:/tmp/CSC469A1/top$ ls
```

```
greywolf:/tmp/CSC469A1/top$ cd ...
```

**Post LS:**

File: `top'

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 809h/2057d Inode: 136274 Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandrr) Gid: ( 1009/gstudent)

Access: 2011-10-02 18:07:56.000000000 -0400

Modify: 2011-10-02 18:03:37.000000000 -0400

Change: 2011-10-02 18:03:37.000000000 -0400

**Pre Chmod:**

File: `f2'

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: 809h/2057d Inode: 136300 Links: 1

Access: (0600/-rw-----) Uid: (10020/g9chandrr) Gid: ( 1009/gstudent)

Access: 2011-10-02 19:42:11.000000000 -0400

Modify: 2011-10-02 19:42:11.000000000 -0400

Change: 2011-10-02 19:42:11.000000000 -0400

```
greywolf:/tmp/CSC469A1$ touch f2
```

```
greywolf:/tmp/CSC469A1$ chmod u-w f2
```

**Post Chmod**

File: `f2'

Size: 0 Blocks: 0 IO Block: 4096 regular empty file



Device: 809h/2057d Inode: 136300 Links: 1  
Access: (0700/-rwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-02 19:42:11.000000000 -0400  
Modify: 2011-10-02 19:42:11.000000000 -0400  
Change: 2011-10-02 19:44:46.000000000 -0400

**Pre failed write operation due to Chmod change:**

greywolf:/tmp/CSC469A1/ND/subND\$ chmod u-w file

greywolf:/tmp/CSC469A1/ND/subND\$ stat file

File: `file`

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: 809h/2057d Inode: 136313 Links: 1  
Access: (0400/-r-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:23:02.000000000 -0400  
Modify: 2011-10-03 14:23:02.000000000 -0400  
Change: 2011-10-03 14:23:16.000000000 -0400

greywolf:/tmp/CSC469A1/ND/subND\$ echo "DFAS">> file

-bash: file: Permission denied

**Post failed write operation due to Chmod change:**

greywolf:/tmp/CSC469A1/ND/subND\$ stat file

File: `file`

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: 809h/2057d Inode: 136313 Links: 1  
Access: (0400/-r-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:23:02.000000000 -0400  
Modify: 2011-10-03 14:23:02.000000000 -0400  
Change: 2011-10-03 14:23:16.000000000 -0400

**Pre: Chmod on directory ( also files inside directory perspective)**

greywolf:/tmp/CSC469A1/ND/subND\$ stat file2

File: `file2`

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: 809h/2057d Inode: 136314 Links: 1  
Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:26:15.000000000 -0400  
Modify: 2011-10-03 14:26:15.000000000 -0400  
Change: 2011-10-03 14:26:15.000000000 -0400

greywolf:/tmp/CSC469A1/ND/subND\$ cd ..; stat subND

File: `subND`

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 809h/2057d Inode: 136312 Links: 2  
Access: (0700/drwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:26:08.000000000 -0400  
Modify: 2011-10-03 14:26:15.000000000 -0400  
Change: 2011-10-03 14:26:15.000000000 -0400

**Post: Chmod on directory ( also files inside directory perspective)**

greywolf:/tmp/CSC469A1/ND\$ stat subND; chmod u-w subND

File: `subND'

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 809h/2057d Inode: 136312 Links: 2  
Access: (0700/drwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:26:08.000000000 -0400  
Modify: 2011-10-03 14:26:15.000000000 -0400  
Change: 2011-10-03 14:27:17.000000000 -0400

greywolf:/tmp/CSC469A1/ND\$ cd subND

greywolf:/tmp/CSC469A1/ND/subND\$ stat file2

File: `file2'

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: 809h/2057d Inode: 136314 Links: 1  
Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:26:15.000000000 -0400  
Modify: 2011-10-03 14:26:15.000000000 -0400  
Change: 2011-10-03 14:26:15.000000000 -0400

**pre: TOUCHING (directory perspective)**

greywolf:/tmp/CSC469A1/top\$ stat sub1

File: `sub1'

Size: 4096 Blocks: 8 IO Block: 4096 directory

Device: 809h/2057d Inode: 136293 Links: 2  
Access: (0700/drwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-02 19:31:10.000000000 -0400  
Modify: 2011-10-02 19:31:06.000000000 -0400  
Change: 2011-10-02 19:31:06.000000000 -0400

drwx----- 3 g9chandr gstudent 4096 Oct 2 19:33 sub1

greywolf:/tmp/CSC469A1/top/sub1\$ cd sub1

greywolf:/tmp/CSC469A1/top\$ cd touch fl

greywolf:/tmp/CSC469A1/top/sub1\$ cd ..

**post: TOUCHING**

greywolf:/tmp/CSC469A1/top/sub1\$ stat .

```
File: `.'
Size: 4096      Blocks: 8      IO Block: 4096  directory
Device: 809h/2057d  Inode: 136293  Links: 3
Access: (0700/drwx-----)  Uid: (10020/g9chandr)  Gid: ( 1009/gstudent)
Access: 2011-10-02 19:31:10.000000000 -0400
Modify: 2011-10-02 19:42:11.000000000 -0400
Change: 2011-10-02 19:42:11.000000000 -0400
drwx----- 3 g9chandr gstudent 4096 Oct  2 19:42 sub1
```

### **pre: Echo (file perspective)**

```
greywolf:~/Courses/CSC469/A1/A1FileRepo/subDir$ stat file1
File: `file1'
Size: 0      Blocks: 0      IO Block: 8192  regular empty file
Device: 1bh/27d Inode: 7791812  Links: 1
Access: (0600/-rw-----)  Uid: (10020/g9chandr)  Gid: ( 1009/gstudent)
Access: 2011-09-30 16:58:59.000000000 -0400
Modify: 2011-09-30 16:58:59.000000000 -0400
Change: 2011-09-30 16:58:59.000000000 -0400
-rw----- 1 g9chandr gstudent 19 Oct  2 17:24 file2
greywolf:~/Courses/CSC469/A1/A1FileRepo/subDir$ echo "TEST" >> file1
```

### **post Echo:**

```
Size: 76      Blocks: 0      IO Block: 8192  regular file
Device: 1bh/27d Inode: 7791812  Links: 1
Access: (0600/-rw-----)  Uid: (10020/g9chandr)  Gid: ( 1009/gstudent)
Access: 2011-09-30 16:58:59.000000000 -0400
Modify: 2011-09-30 17:24:34.000000000 -0400
Change: 2011-09-30 17:24:34.000000000 -0400
-rw----- 1 g9chandr gstudent 19 Oct  2 17:24 file2
```

### **Pre Cat:**

```
File: `file1'
Size: 0      Blocks: 0      IO Block: 4096  regular empty file
Device: 809h/2057d  Inode: 136306  Links: 1
Access: (0600/-rw-----)  Uid: (10020/g9chandr)  Gid: ( 1009/gstudent)
Access: 2011-10-02 19:50:40.000000000 -0400
Modify: 2011-10-02 19:50:40.000000000 -0400
Change: 2011-10-02 19:50:40.000000000 -0400
greywolf:~/Courses/CSC469/A1/A1FileRepo/subDir$ cat file1
```

**Post Cat:**

File: `file1`

Size: 0            Blocks: 0            IO Block: 4096   regular empty file

Device: 809h/2057d    Inode: 136306    Links: 1

Access: (0600/-rw-----) Uid: (10020/g9chandr)    Gid: ( 1009/gstudent)

Access: 2011-10-02 20:13:24.000000000 -0400

Modify: 2011-10-02 19:50:40.000000000 -0400

Change: 2011-10-02 19:50:40.000000000 -0400

**Pre cp of file (FROM DIRECORY PERSPECTIVES):**

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR\$ cd sub1

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR/sub1\$ touch file

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR/sub1\$ cd ..

**SOURCE**

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR\$ stat sub1

File: `sub1`

Size: 4096            Blocks: 8            IO Block: 4096   directory

Device: 809h/2057d    Inode: 136327    Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandr)    Gid: ( 1009/gstudent)

Access: 2011-10-03 15:29:51.000000000 -0400

Modify: 2011-10-03 15:35:35.000000000 -0400

Change: 2011-10-03 15:35:35.000000000 -0400

**DESTINATION**

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR\$ stat sub2

File: `sub2`

Size: 4096            Blocks: 8            IO Block: 4096   directory

Device: 809h/2057d    Inode: 136328    Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandr)    Gid: ( 1009/gstudent)

Access: 2011-10-03 15:31:13.000000000 -0400

Modify: 2011-10-03 15:31:36.000000000 -0400

Change: 2011-10-03 15:31:36.000000000 -0400

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR\$ cp sub1/file sub2/

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR\$ stat sub2

**Post cp of file (FROM DIRECORY PERSPECTIVES):**

**SOURCE**

greywolf:/tmp/CSC469A1/ND/NDir2/testDIR\$ stat sub1

File: `sub1'

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136327   Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 15:35:54.000000000 -0400

Modify: 2011-10-03 15:35:35.000000000 -0400

Change: 2011-10-03 15:35:35.000000000 -0400

**DESTINATION**

File: `sub2'

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136328   Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 15:31:13.000000000 -0400

Modify: 2011-10-03 15:35:58.000000000 -0400

Change: 2011-10-03 15:35:58.000000000 -0400

PRE CP OF A FILE

**Pre cp of file (FROM FILE PERSPECTIVES):**

**FILE (source):**

File: `f3'

Size: 0      Blocks: 0      IO Block: 4096   regular empty file

Device: 809h/2057d   Inode: 136287   Links: 1

Access: (0600/-rw-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-02 18:16:55.000000000 -0400

Modify: 2011-10-02 18:16:55.000000000 -0400

Change: 2011-10-02 18:16:55.000000000 -0400

greywolf:/tmp/CSC469A1\$ cp f3 top

greywolf:/tmp/CSC469A1\$ stat f3

File: `f3'

Size: 0      Blocks: 0      IO Block: 4096   regular empty file

Device: 809h/2057d   Inode: 136287   Links: 1

Access: (0600/-rw-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-02 18:18:36.000000000 -0400

Modify: 2011-10-02 18:16:55.000000000 -0400

Change: 2011-10-02 18:16:55.000000000 -0400

**Pre cp of file (FROM FILE PERSPECTIVES):**

**FILE (SOURCE):**

greywolf:/tmp/CSC469A1/top\$ stat f3

File: `f3'

Size: 0            Blocks: 0            IO Block: 4096   regular empty file

Device: 809h/2057d   Inode: 136289   Links: 1

Access: (0600/-rw-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-02 18:18:35.000000000 -0400

Modify: 2011-10-02 18:18:35.000000000 -0400

Change: 2011-10-02 18:18:35.000000000 -0400

*without overwrite (no change, output truncated)*

*with overwrite:*

*File (original)*

*same behavior*

*file (destination Overwritten)*

greywolf:/tmp/CSC469A1/top\$ stat f3

File: `f3'

Size: 0            Blocks: 0            IO Block: 4096   regular empty file

Device: 809h/2057d   Inode: 136289   Links: 1

Access: (0600/-rw-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-02 18:18:35.000000000 -0400

Modify: 2011-10-02 18:18:35.000000000 -0400

Change: 2011-10-02 18:18:35.000000000 -0400

-rw----- 1 g9chandr gstudent 0 Oct 2 18:18:35.000000000 file2

greywolf:/tmp/CSC469A1/top\$ stat f3

File: `f3'

Size: 0            Blocks: 0            IO Block: 4096   regular empty file

Device: 809h/2057d   Inode: 136289   Links: 1

Access: (0600/-rw-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-02 18:18:35.000000000 -0400

Modify: 2011-10-02 18:21:05.000000000 -0400

Change: 2011-10-02 18:21:05.000000000 -0400

-rw----- 1 g9chandr gstudent 0 Oct 2 18:21 file2

**pre: Sub directory creation( parent directory perspective)**

File: `DIR'

Size: 4096            Blocks: 8            IO Block: 4096   directory

Device: 809h/2057d Inode: 136304 Links: 3  
Access: (0700/drwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-02 20:06:33.000000000 -0400  
Modify: 2011-10-02 20:06:59.000000000 -0400  
Change: 2011-10-02 20:06:59.000000000 -0400  
drwx----- 3 g9chandr gstudent 4096 Oct 2 20:06 DIR

greywolf:/tmp/CSC469A1/top\$ cd DIR  
greywolf:/tmp/CSC469A1/top/DIR\$ mkdir sub1

**Post: sub directory creation:**

File: `DIR'  
Size: 4096 Blocks: 8 IO Block: 4096 directory  
Device: 809h/2057d Inode: 136304 Links: 4  
Access: (0700/drwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-02 20:08:18.000000000 -0400 **(NOTE: the time updated here due to an ls, examine the times and one can see the same action did not cause the update as the action that updated modified and changed)**  
Modify: 2011-10-02 20:08:29.000000000 -0400  
Change: 2011-10-02 20:08:29.000000000 -0400  
drwx----- 3 g9chandr gstudent 4096 Oct 2 20:08 DIR

**Pre wc**

File: `file2'  
Size: 0 Blocks: 0 IO Block: 4096 regular empty file  
Device: 809h/2057d Inode: 136308 Links: 1  
Access: (0700/-rwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-02 19:56:13.000000000 -0400  
Modify: 2011-10-02 20:26:03.000000000 -0400  
Change: 2011-10-02 20:26:03.000000000 -0400  
-rwx----- 1 g9chandr gstudent 0 Oct 2 20:26 file2  
greywolf:/tmp/CSC469A1/top\$ wc file2

**Post wc**

File: `file2'  
Size: 0 Blocks: 0 IO Block: 4096 regular empty file  
Device: 809h/2057d Inode: 136308 Links: 1  
Access: (0700/-rwx-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-02 20:40:32.000000000 -0400  
Modify: 2011-10-02 20:26:03.000000000 -0400  
Change: 2011-10-02 20:26:03.000000000 -0400

**pre: creation of file within subdirectory (perspective of parent directory)**

greywolf:/tmp/CSC469A1\$ stat ND

File: `ND`

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136311   Links: 3

Access: (0700/drwx-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 13:42:23.000000000 -0400

Modify: 2011-10-03 13:42:37.000000000 -0400

Change: 2011-10-03 13:42:37.000000000 -0400

greywolf:/tmp/CSC469A1\$ CD ND

greywolf:/tmp/CSC469A1\$ touch file1

**post: creation of file within subdirectory (perspective of parent directory)**

File: `ND`

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136311   Links: 3

Access: (0700/drwx-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 13:42:23.000000000 -0400

Modify: 2011-10-03 13:42:37.000000000 -0400

Change: 2011-10-03 13:42:37.000000000 -0400

**pre: Deletion of a file within a directory (parent directory view)**

greywolf:/tmp/CSC469A1/ND\$ stat subND

File: `subND`

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136312   Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 13:42:53.000000000 -0400

Modify: 2011-10-03 13:42:55.000000000 -0400

Change: 2011-10-03 13:42:55.000000000 -0400

greywolf:/tmp/CSC469A1/ND/subND\$ rm -rf file

**post: Deletion of a file within a directory (parent directory view)**

File: `subND`

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136312   Links: 2

Access: (0700/drwx-----) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 13:42:53.000000000 -0400

Modify: 2011-10-03 13:55:05.000000000 -0400

Change: 2011-10-03 13:55:05.000000000 -0400



**pre:Deletion of a file within a directory (parent of parent directory view):**

greywolf:/tmp/CSC469A1\$ stat ND

File: 'ND'

Size: 4096      Blocks: 8      IO Block: 4096    directory

Device: 809h/2057d    Inode: 136311    Links: 3

Access: (0700/drwx-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 13:54:10.000000000 -0400

Modify: 2011-10-03 13:42:37.000000000 -0400

Change: 2011-10-03 13:42:37.000000000 -0400

greywolf:/tmp/CSC469A1/ND/subND\$ rm -rf file

**post:Deletion of a file within a directory (parent of parent directory perspective):**

File: 'ND'

Size: 4096      Blocks: 8      IO Block: 4096    directory

Device: 809h/2057d    Inode: 136311    Links: 3

Access: (0700/drwx-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 13:54:10.000000000 -0400

Modify: 2011-10-03 13:42:37.000000000 -0400

Change: 2011-10-03 13:42:37.000000000 -0400

**Pre: Succesful directory removal (parent of directory to be deleted perspective)**

greywolf:/tmp/CSC469A1\$ stat ND

File: 'ND'

Size: 4096      Blocks: 8      IO Block: 4096    directory

Device: 809h/2057d    Inode: 136311    Links: 4

Access: (0700/drwx-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 14:09:28.000000000 -0400

Modify: 2011-10-03 14:00:03.000000000 -0400

Change: 2011-10-03 14:00:03.000000000 -0400

greywolf:/tmp/CSC469A1/ND\$ rmdir subND2

**Post: Succesful directory removal (parent of directory to be deleted perspective)**

greywolf:/tmp/CSC469A1\$ stat ND

File: 'ND'

Size: 4096      Blocks: 8      IO Block: 4096    directory

Device: 809h/2057d    Inode: 136311    Links: 3

Access: (0700/drwx-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 14:09:28.000000000 -0400

Modify: 2011-10-03 14:09:56.000000000 -0400

Change: 2011-10-03 14:09:56.000000000 -0400

**Pre: failed directory removal (parent of directory to be deleted perspective)**

greywolf:/tmp/CSC469A1\$ stat ND

File: `ND`

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136311   Links: 4

Access: (0700/drwx-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 14:01:06.000000000 -0400

Modify: 2011-10-03 14:00:03.000000000 -0400

Change: 2011-10-03 14:00:03.000000000 -0400

greywolf:/tmp/CSC469A1/ND\$ rmdir subND2

rmdir: failed to remove `subND2': Directory not empty

**Post: failed directory removal (parent of directory to be deleted perspective):**

greywolf:/tmp/CSC469A1/ND\$ stat subND2

File: `subND2`

Size: 4096      Blocks: 8      IO Block: 4096   directory

Device: 809h/2057d   Inode: 136313   Links: 2

Access: (0700/drwx-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 14:00:03.000000000 -0400

Modify: 2011-10-03 14:00:33.000000000 -0400

Change: 2011-10-03 14:00:33.000000000 -0400

**Pre: hard link (file being linked to perspective)**

greywolf:/tmp/CSC469A1/ND/NDir2\$ stat fl

File: `fl`

Size: 0      Blocks: 0      IO Block: 4096   regular empty file

Device: 809h/2057d   Inode: 136317   Links: 1

Access: (0600/-rw-----)   Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 14:30:24.000000000 -0400

Modify: 2011-10-03 14:30:24.000000000 -0400

Change: 2011-10-03 14:30:24.000000000 -0400

greywolf:/tmp/CSC469A1/ND/NDir2\$ cd ../NDir

greywolf:/tmp/CSC469A1/ND/NDir\$ ln ../NDir2/fl flHardLink

**Post: hard link (file being linked to perspective)**

greywolf:/tmp/CSC469A1/ND/NDir2\$ stat fl

File: `fl`

Size: 0            Blocks: 0            IO Block: 4096   regular empty file  
Device: 809h/2057d   Inode: 136317   Links: 2  
Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:30:24.000000000 -0400  
Modify: 2011-10-03 14:30:24.000000000 -0400  
Change: 2011-10-03 14:32:02.000000000 -0400

**Pre: File Hard link linked to deleted (hard link perspective):**

greywolf:/tmp/CSC469A1/ND/NDir\$ stat f1HardLink

File: `f1HardLink'

Size: 0            Blocks: 0            IO Block: 4096   regular empty file  
Device: 809h/2057d   Inode: 136317   Links: 2  
Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:30:24.000000000 -0400  
Modify: 2011-10-03 14:30:24.000000000 -0400  
Change: 2011-10-03 14:32:02.000000000 -0400

greywolf:/tmp/CSC469A1/ND/NDir2\$ rm -rf f1

**Post: File Hard link linked to deleted (hard link perspective):**

greywolf:/tmp/CSC469A1/ND/NDir\$ stat f1HardLink

File: `f1HardLink'

Size: 0            Blocks: 0            IO Block: 4096   regular empty file  
Device: 809h/2057d   Inode: 136317   Links: 1  
Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:30:24.000000000 -0400  
Modify: 2011-10-03 14:30:24.000000000 -0400  
Change: 2011-10-03 14:35:53.000000000 -0400

**Pre: File Hard link linked to updated (hard link perspective):**

greywolf:/tmp/CSC469A1/ND/NDir\$ ln ../NDir2/f2 f2HardLink

greywolf:/tmp/CSC469A1/ND/NDir\$ stat f2HardLink

File: `f2HardLink'

Size: 0            Blocks: 0            IO Block: 4096   regular empty file  
Device: 809h/2057d   Inode: 136318   Links: 2  
Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 14:39:11.000000000 -0400  
Modify: 2011-10-03 14:39:11.000000000 -0400  
Change: 2011-10-03 14:39:21.000000000 -0400

greywolf:/tmp/CSC469A1/ND/NDir2\$ echo "test" >> f2

**Post: File Hard link linked to updated (hard link perspective):**

greywolf:/tmp/CSC469A1/ND/NDir\$ stat f2HardLink

File: `f2HardLink'

Size: 5 Blocks: 8 IO Block: 4096 regular file

Device: 809h/2057d Inode: 136318 Links: 2

Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)

Access: 2011-10-03 14:39:11.000000000 -0400

Modify: 2011-10-03 14:39:50.000000000 -0400

Change: 2011-10-03 14:39:50.000000000 -0400

**Pre: Soft link (file being linked to perspective):**

greywolf:/tmp/CSC469A1/ND/NDir2\$ touch f4

greywolf:/tmp/CSC469A1/ND/NDir2\$ stat f4

File: `f4'

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: 809h/2057d Inode: 136321 Links: 1

Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)

Access: 2011-10-03 14:49:10.000000000 -0400

Modify: 2011-10-03 14:49:10.000000000 -0400

Change: 2011-10-03 14:49:10.000000000 -0400

greywolf:/tmp/CSC469A1/ND/NDir\$ ln -s ../NDir2/f4 f4SymLink

**Post: Soft link (file being linked to perspective):**

greywolf:/tmp/CSC469A1/ND/NDir2\$ stat f4

File: `f4'

Size: 0 Blocks: 0 IO Block: 4096 regular empty file

Device: 809h/2057d Inode: 136321 Links: 1

Access: (0600/-rw-----) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)

Access: 2011-10-03 14:49:10.000000000 -0400

Modify: 2011-10-03 14:49:10.000000000 -0400

Change: 2011-10-03 14:49:10.000000000 -0400

**Pre: File Soft link linked to updated ( Soft link perspective):**

greywolf:/tmp/CSC469A1/ND/NDir\$ stat f4SymLink

File: `f4SymLink' -> `../NDir2/f4'

Size: 11 Blocks: 0 IO Block: 4096 symbolic link

Device: 809h/2057d Inode: 136322 Links: 1

Access: (0777/lrwxrwxrwx) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Modify: 2011-10-03 14:57:02.000000000 -0400  
Modify: 2011-10-03 14:57:02.000000000 -0400  
Change: 2011-10-03 14:57:02.000000000 -0400  
greywolf:/tmp/CSC469A1/ND/NDir2\$ echo "test">>f4

**Post: File Soft link linked to updated ( Soft link perspective):**

greywolf:/tmp/CSC469A1/ND/NDir\$ stat f4SymLink  
File: `f4SymLink' -> `../NDir2/f4'  
Size: 11 Blocks: 0 IO Block: 4096 symbolic link  
Device: 809h/2057d Inode: 136322 Links: 1  
Access: (0777/lrwxrwxrwx) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 15:00:54.000000000 -0400 (**result of stat command**)  
Modify: 2011-10-03 14:57:02.000000000 -0400  
Change: 2011-10-03 14:57:02.000000000 -0400

**Pre: File Soft link linked to deleted (hard link perspective):**

greywolf:/tmp/CSC469A1/ND/NDir\$ stat f4SymLink  
File: `f4SymLink' -> `../NDir2/f4'  
Size: 11 Blocks: 0 IO Block: 4096 symbolic link  
Device: 809h/2057d Inode: 136322 Links: 1  
Access: (0777/lrwxrwxrwx) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 15:10:48.000000000 -0400  
Modify: 2011-10-03 14:57:02.000000000 -0400  
Change: 2011-10-03 14:57:02.000000000 -0400

greywolf:/tmp/CSC469A1/ND/NDir2\$ rm -rf f5

**Post: File Soft link linked to deleted (hard link perspective):**

File: `f4SymLink' -> `../NDir2/f4'  
Size: 11 Blocks: 0 IO Block: 4096 symbolic link  
Device: 809h/2057d Inode: 136322 Links: 1  
Access: (0777/lrwxrwxrwx) Uid: (10020/g9chandr) Gid: ( 1009/gstudent)  
Access: 2011-10-03 15:10:49.000000000 -0400  
Modify: 2011-10-03 14:57:02.000000000 -0400  
Change: 2011-10-03 14:57:02.000000000 -0400

**Post: Stat on soft link ( Soft link perspective):**

File: `f4SymLink' -> `../NDir2/f4'

Size: 11      Blocks: 0      IO Block: 4096   symbolic link

Device: 809h/2057d    Inode: 136322    Links: 1

Access: (0777/lrwxrwxrwx) Uid: (10020/g9chandr)   Gid: ( 1009/gstudent)

Access: 2011-10-03 15:12:15.000000000 -0400

Modify: 2011-10-03 14:57:02.000000000 -0400

Change: 2011-10-03 14:57:02.000000000 -0400