

# Computer Forensics

## Part 1 : File carving

1. Look at the data on the file system (Click on Data Sources and look at the hex values on the right).

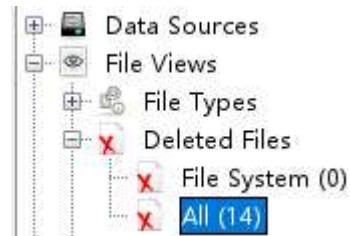
The file system has no files, but why are we able to find items on the disk image? Explain why the file system has no files but there are items that can be found on the disk image.

Ans : Because the files were deleted but not overwritten yet. The file system marks their space as unallocated, so it appears empty, but the contents still exist on the disk. Autopsy has capability to read directly from the disk image.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
f0000281_Nick_is_a.pretty_man.with_a_2003_d4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19968	Unallocated
f0000321.wmv				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8037267	Unallocated
f0016021.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	318894	Unallocated
f0016693.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23040	Unallocated
f0016741_Prudent_Engineering_Practice_for_Cr	▼	0		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1399508	Unallocated
f0019477.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	122434	Unallocated
f0019717.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29885	Unallocated
f0019777.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	444314	Unallocated
f0020645.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	99298	Unallocated
f0020841.gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5498	Unallocated
f0020853_moov.mov				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	550653	Unallocated
f0021929.wmv				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1036994	Unallocated
f0023957.ppt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11264	Unallocated
f0023981_vvword60.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	78899	Unallocated

2. How many objects can you find?

Ans : 14 objects



**3. List all the objects here and report on whether or not the content is accessible or damaged/corrupted. Also note which files were actually already deleted.**

Ans : Since every file shows an “unallocated” flag, it means every file is already deleted. But every file is still accessible.

Here are some examples. others files I check through extract and open it in local



**4. Think securely: If we want to delete files on a magnetic hard disk and not have them be recovered by any tool, what do we need to do? And how much time do you think you need to wipe a 1TB magnetic hard disk?**

Ans : Based on Q1 the reason is “files were deleted but not over written yet”, so what we need to do is overwrite it with any data, time usage is fully based on the disk write speed, lets said 150 MB/s (avg HDD write speed) it will take around 1.85 hours.

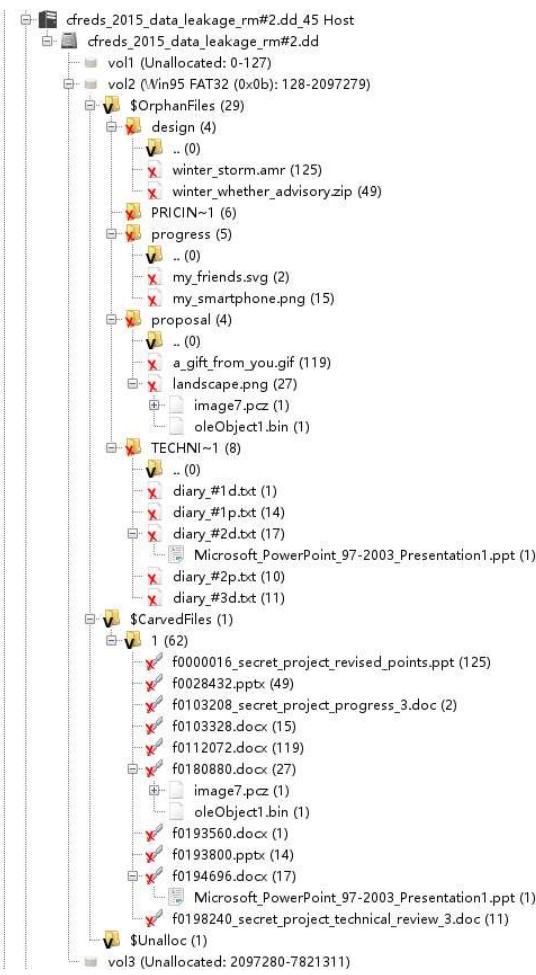
**5. Will file carving be able to recover deleted files on an SSD? Why or why not?**

Ans : Nope, while HDDs keep deleted data until overwritten, SSDs actively clear it after TRIM. As a result, carving tools find nothing left to reconstruct.

## **Part 2 : Investigation**

**1. List all directories that were traversed in ‘RM#2’.**

Ans : Picture shows below



## 2. List all files that were opened in 'RM#2'.

Ans : Showing below, Only filter file accessed operation

The screenshot shows a timeline editor interface with the following configuration:

- Timeline - Editor**
- Display Times In:** Local Time Zone / GMT / UTC
- View Mode:** Counts, Details, List (selected)
- Filters:**
  - Must include text: enter filter string
  - Must be tagged
  - Must have hash hit
  - Limit data sources to:
    - forensics-p2.dd (ID: 1)
    - cfred's\_2015\_data\_leakage...
  - Limit file types to:
    - Media
    - Documents
    - Executables
    - Other
  - Limit event types to:
    - File System
      - File Accessed
      - File Changed
      - File Created
      - File Modified
    - Web Activity
      - Web Bookmarks
      - Web Cache
      - Web Cookies Accessed
      - Web Cookies Create
      - Web Downloads
      - Web Form Address Create...
      - Web Form Address Modify...
- Event List:**

Date/Time	Event Type	Description	Tagged	Hash Hit
2015-03-23 00:00:00	A__	/\$OrphanFiles/staps.gif		
2015-03-23 00:00:00	A__	/\$OrphanFiles/boudicca.bmp		
2015-03-23 00:00:00	A__	/\$OrphanFiles/FORSYT-1.PNG		
2015-03-23 00:00:00	A__	/\$OrphanFiles/barn.gif		
2015-03-23 00:00:00	A__	/\$OrphanFiles/plAZZA-1.JPG		
2015-03-23 00:00:00	A__	/\$OrphanFiles/jump.jpg		
2015-03-23 00:00:00	A__	/\$OrphanFiles/JACK-O-1.TIF		
2015-03-23 00:00:00	A__	/\$OrphanFiles/pisa.JPG		
2015-03-23 00:00:00	A__	/\$OrphanFiles/CUTTY--1.JPG		
2015-03-23 00:00:00	A__	/\$OrphanFiles/mafla.bmp		
2015-03-23 00:00:00	A__	/\$OrphanFiles/wat.gif		
2015-03-23 00:00:00	A__	/\$OrphanFiles/leaf.jpg		
2015-03-23 00:00:00	A__	/\$OrphanFiles/BAMBOO-1.GIF		
2015-03-23 00:00:00	A__	/\$OrphanFiles/nigeria.gif		
2015-03-23 00:00:00	A__	/\$OrphanFiles/cactus.png		
2015-03-23 00:00:00	A__	/\$OrphanFiles/STONH-1.JPG		
2015-03-23 00:00:00	A__	/\$OrphanFiles/eggs.gif		
2015-03-23 00:00:00	A__	/\$OrphanFiles/tomatoes.gif		
2015-03-23 00:00:00	A__	/\$OrphanFiles/snow-snow.jpg		
2015-03-23 00:00:00	A__	/\$OrphanFiles/save.png		
2015-03-23 00:00:00	A__	/\$OrphanFiles/orchid.png		
2015-03-23 00:00:00	A__	/\$OrphanFiles/SPQR.JPG		
2015-03-23 00:00:00	A__	/\$OrphanFiles/blini.gif		
2015-03-24 00:00:00	A__	/\$OrphanFiles/PRICIN=1/new_years_day.jpg		
2015-03-24 00:00:00	A__	/\$OrphanFiles/PRICIN=1/my_favorite_movies.7z		
2015-03-24 00:00:00	A__	/\$OrphanFiles/design/winter_weather_advisory.zip		
2015-03-24 00:00:00	A__	/\$OrphanFiles/TECHNI-1		
2015-03-24 00:00:00	A__	/\$OrphanFiles/design/winter_storm.amr		

Filters		View Mode:		Counts	Details	List	Add Event	Snapshot Report	Refresh View
<input type="checkbox"/> History	<input type="button"/> Back	<input type="button"/> Forward							
<input type="checkbox"/> Must include text <input type="text" value="enter filter string"/>									
<input type="checkbox"/> Must be tagged									
<input type="checkbox"/> Must have hash hit									
<input type="checkbox"/> Limit data sources to									
<input type="checkbox"/> forensics.p2p.dd (0:1)									
<input type="checkbox"/> cfredis2015_data_leakage...									
<input type="checkbox"/> Limit file types to									
<input checked="" type="checkbox"/> Media									
<input checked="" type="checkbox"/> Documents									
<input checked="" type="checkbox"/> Executables									
<input checked="" type="checkbox"/> Other									
<input checked="" type="checkbox"/> Limit event types to									
<input checked="" type="checkbox"/> File System									
<input checked="" type="checkbox"/> File Accessed									
<input type="checkbox"/> File Changed									
<input type="checkbox"/> File Created									
<input type="checkbox"/> File Modified									
<input checked="" type="checkbox"/> Web Activity									
<input checked="" type="checkbox"/> Web Bookmarks									
<input checked="" type="checkbox"/> Web Cache									
<input checked="" type="checkbox"/> Web Cookies Accessed									
<input checked="" type="checkbox"/> Web Cookies Create									
<input checked="" type="checkbox"/> Web Downloads									
<input checked="" type="checkbox"/> Web Form Address Create...									
<input checked="" type="checkbox"/> Web Form Address Modifi...									

### 3. Recover deleted files from USB drive 'RM#2'. What files were you able to recover?

Ans :

Directory tree		Using									
		All									
		Table Thumbnail Summary									
		Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
		f0000281_Nick_is_a.pretty_man.with_a_2003_dc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19988	Unallocated
		f0000321.wmv				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8037267	Unallocated
		f0010201.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	318894	Unallocated
		f0016693.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23040	Unallocated
		f0017471_Proudent_Engineering_Practice_for_Cn	D			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	139950	Unallocated
		f0018477.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	122434	Unallocated
		f0019777.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29885	Unallocated
		f0020645.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	93298	Unallocated
		f0020841.gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5489	Unallocated
		f0020853.mov.mov				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	550653	Unallocated
		f0021929.wmv				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1036994	Unallocated
		f0023957.ppt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11264	Unallocated
		f0023981_word60.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	78899	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023957.ppt				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated
		f0023981_word60.zip				2015-03-24 09:57:14 ICT	2015-03-24 00:00:00	2015-03-24 00:00:00	2015-03-24 09:59:26 ICT	4096	Unallocated</td

## 5. Recover hidden files from the CD-R ‘RM#3’. What files were you able to recover?

Ans : these 15 files

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0001308_secret_project_revised_points.ppt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14547968	Unallocated	Unknown	/img.dre	
f0029724.pptx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16381123	Unallocated	Unknown	/img.dre	
f0061720_secret_project_price_analysis_2.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1260544	Unallocated	Unknown	/img.dre	
f0064184.xlsx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	100078	Unallocated	Unknown	/img.dre	
f0064380.xlsx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10237552	Unallocated	Unknown	/img.dre	
f0084376_secret_project_market_shares.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10289152	Unallocated	Unknown	/img.dre	
f0104472_secret_project_progress_3.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5734	Unallocated	Unknown	/img.dre	
f0104588.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4440235	Unallocated	Unknown	/img.dre	
f0113264.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	27414	Unallocated	Unknown	/img.dre	
f0198632.xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1531	Unallocated	Unknown	/img.dre	
f0199536_secret_project_technical_review_3.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2360832	Unallocated	Unknown	/img.dre	
f0204148_secret_project_technical_review_3.ppt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	325120	Unallocated	Unknown	/img.dre	
f0205596.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	780831	Unallocated	Unknown	/img.dre	
f0207124.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	777835	Unallocated	Unknown	/img.dre	
f0208644.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	620888	Unallocated	Unknown	/img.dre	

## 6. What actions were performed for anti-forensics (data hiding) on CD-R ‘RM#3’?

Ans : 1. Delete files and 2. Change to random name so even recover can not easily said its leak sensitive

information