Phatcharapon Jumruspun 6031040921

Activity XII: Computer Forensics Part II

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

Date/Time	Description	Event Type
24/3/2015 17:02	/IAMAN $_@ (Volume Label Entry)	File Modified
24/3/2015 9:57	/$OrphanFiles/design	File Modified
24/3/2015 9:57	/$OrphanFiles/PRICIN~1	File Modified
24/3/2015 9:54	/$OrphanFiles/progress	File Modified
24/3/2015 9:55	/$OrphanFiles/proposal	File Modified
24/3/2015 9:56	/$OrphanFiles/TECHNI~1	File Modified

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

Date/Time	Description	Event Type
24/3/2015 10:00	/$OrphanFiles/TECHNI~1/diary_#3p.txt	File Created
24/3/2015 17:02	/IAMAN $_@ (Volume Label Entry)	File Modified
24/3/2015 15:51	/$OrphanFiles/desktop.ini	File Created
24/3/2015 9:59	/$OrphanFiles/design/winter_storm.amr	File Created
24/3/2015 15:51	/$OrphanFiles/desktop.ini	File Modified
24/3/2015 9:59	/$OrphanFiles/design/winter_whether_advisory.zip	File Created
24/3/2015 9:59	/$OrphanFiles/PRICIN~1/my_favorite_cars.db	File Created
24/3/2015 9:59	/$OrphanFiles/PRICIN~1/my_favorite_movies.7z	File Created
24/3/2015 9:59	/$OrphanFiles/PRICIN~1/new_years_day.jpg	File Created
24/3/2015 9:59	/$OrphanFiles/PRICIN~1/super_bowl.avi	File Created
24/3/2015 9:59	/$OrphanFiles/progress/my_friends.svg	File Created
24/3/2015 9:59	/$OrphanFiles/progress/my_smartphone.png	File Created
24/3/2015 9:59	/$OrphanFiles/progress/new_year_calendar.one	File Created
24/3/2015 9:59	/$OrphanFiles/proposal/a_gift_from_you.gif	File Created
24/3/2015 10:00	/$OrphanFiles/proposal/landscape.png	File Created
24/3/2015 10:00	/$OrphanFiles/TECHNI~1/diary_#1d.txt	File Created
24/3/2015 10:00	/$OrphanFiles/TECHNI~1/diary_#1p.txt	File Created
24/3/2015 10:00	/$OrphanFiles/TECHNI~1/diary_#2d.txt	File Created
24/3/2015 10:00	/$OrphanFiles/TECHNI~1/diary_#2p.txt	File Created
24/3/2015 10:00	/$OrphanFiles/TECHNI~1/diary_#3d.txt	File Created

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

Name	Size	Location
f0000000.fat	2048	$CarvedFiles/f0000000.fat
f0000008.fat	2048	$CarvedFiles/f0000008.fat
f0000016_secret_project_revised_points.ppt	14547968	$CarvedFiles/f0000016_secret_project_revised_points.ppt
f0028432.pptx	16381123	$CarvedFiles/f0028432.pptx
f0060432.fat	2048	$CarvedFiles/f0060432.fat
f0060440_secret	1260544	$CarvedFiles/f0060440_secret_project_price_analysis_2.xls

_project_price_analysis_2.xls		
f0062904.xlsx	100078	$CarvedFiles/f0062904.xlsx
f0063104.xlsx	10237535	$CarvedFiles/f0063104.xlsx
f0083104_secret_project_market_shares.xls	10289152	$CarvedFiles/f0083104_secret_project_market_shares.xls
f0103200.fat	2048	$CarvedFiles/f0103200.fat
f0103208_secret_project_progress_3.doc	57344	$CarvedFiles/f0103208_secret_project_progress_3.doc
f0103328.docx	4440235	$CarvedFiles/f0103328.docx
f0112004.mpg	2038	$CarvedFiles/f0112004.mpg
f0112008.docx	27414	$CarvedFiles/f0112008.docx
f0112064.fat	2048	$CarvedFiles/f0112064.fat
f0112072.docx	35226880	$CarvedFiles/f0112072.docx
f0180880.docx	6484502	$CarvedFiles/f0180880.docx
f0193552.fat	2048	$CarvedFiles/f0193552.fat
f0193560.docx	121441	$CarvedFiles/f0193560.docx
f0193800.pptx	458267	$CarvedFiles/f0193800.pptx
f0194696.docx	658922	$CarvedFiles/f0194696.docx
f0197336.xml	1531	$CarvedFiles/f0197336.xml
f0198240_secret_project_technical_review_3.doc	2360832	$CarvedFiles/f0198240_secret_project_technical_review_3.doc
f0202856_secret_project_technical_review_3.ppt	325120	$CarvedFiles/f0202856_secret_project_technical_review_3.ppt
f0203496.fat	2048	$CarvedFiles/f0203496.fat
f0203504.Desktop.ini	129	$CarvedFiles/f0203504.Desktop.ini
f0215936.3gp	11994668	$CarvedFiles/f0215936.3gp
f0239392.3gp	10101908	$CarvedFiles/f0239392.3gp
f0259136.3gp	9024248	$CarvedFiles/f0259136.3gp
f0276768.wma	1293505	$CarvedFiles/f0276768.wma
f0279296.wmv	2467078	$CarvedFiles/f0279296.wmv
f0284128.wmv	4283126	$CarvedFiles/f0284128.wmv
f0292512.wmv	3085265	$CarvedFiles/f0292512.wmv
f0298560_skip.mov	9773451	$CarvedFiles/f0298560_skip.mov
f0317664_skip.mov	590588	$CarvedFiles/f0317664_skip.mov
f0318848.mp4	4949421	$CarvedFiles/f0318848.mp4
f0328544.mp4	885072	$CarvedFiles/f0328544.mp4
f0330304.mp4	15209466	$CarvedFiles/f0330304.mp4
f0360032.fat	2048	$CarvedFiles/f0360032.fat
f0360064.bmp	921654	$CarvedFiles/f0360064.bmp
f0361888.gif	6717692	$CarvedFiles/f0361888.gif

f0375040.gif	3352929	$CarvedFiles/f0375040.gif
f0381600.gif	2125114	$CarvedFiles/f0381600.gif
f0385760.bmp	8798374	$CarvedFiles/f0385760.bmp
f0402976.png	6164389	$CarvedFiles/f0402976.png
f0415040.png	8182655	$CarvedFiles/f0415040.png
f0431040.jpg	1625241	$CarvedFiles/f0431040.jpg
f0434240.gif	2284125	$CarvedFiles/f0434240.gif
f0438720.png	8107995	$CarvedFiles/f0438720.png
f0454560.gif	34480	$CarvedFiles/f0454560.gif
f0454656.tif	7553024	$CarvedFiles/f0454656.tif
f0469408.jpg	2015880	$CarvedFiles/f0469408.jpg
f0473376.jpg	798064	$CarvedFiles/f0473376.jpg
f0474944.jpg	1370140	$CarvedFiles/f0474944.jpg
f0477632.png	8455527	$CarvedFiles/f0477632.png
f0494176.jpg	1267394	$CarvedFiles/f0494176.jpg
f0496672.jpg	847709	$CarvedFiles/f0496672.jpg
f0498336.jpg	897275	$CarvedFiles/f0498336.jpg
f0500096.jpg	1236401	$CarvedFiles/f0500096.jpg
f0502528.gif	2242264	$CarvedFiles/f0502528.gif
f0506912.gif	2240548	$CarvedFiles/f0506912.gif
f0511296.gif	32186	$CarvedFiles/f0511296.gif

4. What actions were performed for anti-forensics on USB drive RM#2?

Overwriting with trash files, as there are a lot of files having to be carved from unallocated areas. Additionally there are a lot of unrelated files implying there were attempts to completely overwrite unallocated blocks of the disk.

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

Name	Size	Location
f0001308_secret_project_revised_points.ppt	14547968	$CarvedFiles/f0001308_secret_project_revised_points.ppt
f0029724.pptx	16381123	$CarvedFiles/f0029724.pptx
f0061720_secret_project_price_analysis_2.xls	1260544	$CarvedFiles/f0061720_secret_project_price_analysis_2.xls
f0064184.xlsx	100078	$CarvedFiles/f0064184.xlsx
f0064380.xlsx	10237535	$CarvedFiles/f0064380.xlsx
f0084376_secret_project_market_shares.xls	10289152	$CarvedFiles/f0084376_secret_project_market_shares.xls
f0104472_secret_project_progress_3.doc	57344	$CarvedFiles/f0104472_secret_project_progress_3.doc
f0104588.docx	4440235	$CarvedFiles/f0104588.docx
f0113264.docx	27414	$CarvedFiles/f0113264.docx
f0198632.xml	1531	$CarvedFiles/f0198632.xml

f0199536_secret _project_technical _review_3.doc	2360832	$CarvedFiles/f0199536_secret_project_technical_review_3.doc
f0204148_secret _project_technical _review_3.ppt	325120	$CarvedFiles/f0204148_secret_project_technical_review_3.ppt
f0205596.jpg	780831	$CarvedFiles/f0205596.jpg
f0207124.jpg	777835	$CarvedFiles/f0207124.jpg
f0208644.jpg	620888	$CarvedFiles/f0208644.jpg

6. What actions were performed for anti-forensics on CD-R RM#3

The tracks left behind is also similar to what we have in RM#2 drive, which are a lot of unrelated files, and also the file carving technique in order to recover the deleted files. So all of this also implied that there were attempts of overwriting unallocated areas.