Computer Security
Dept. of Computer Engineering
Chulalongkorn University

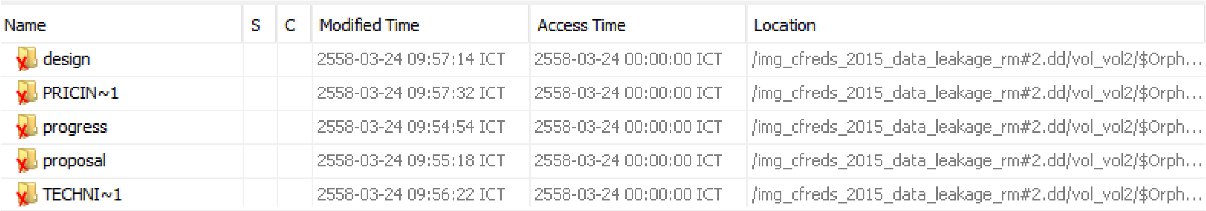
Activity XII : Computer Forensics

Instructors : Kunwadee Sripanidkulchai, Ph.D.

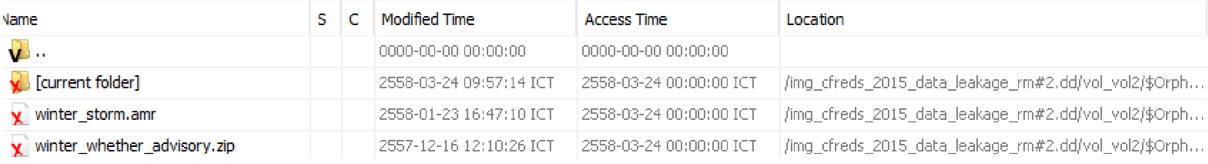
Part II. Investigation

Answer these questions:

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



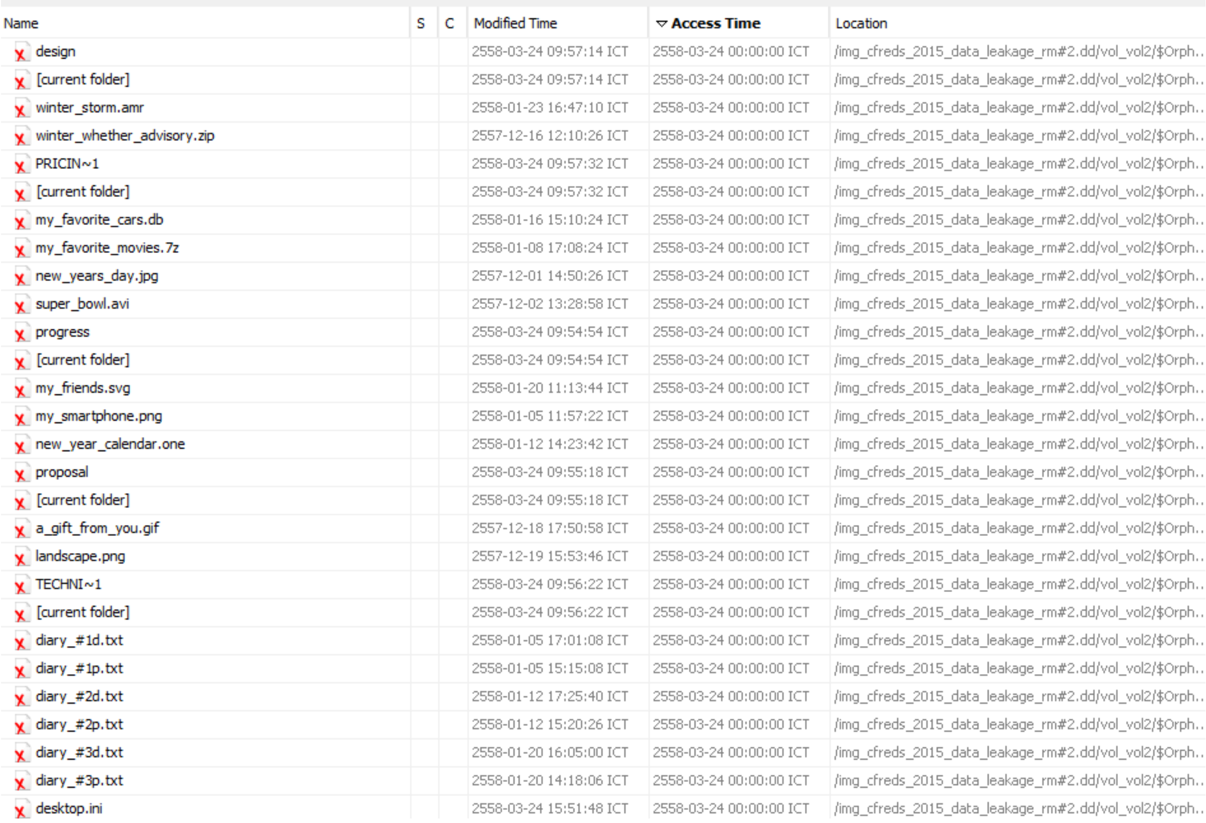
Name	S	C	Modified Time	Access Time	Location
design			2558-03-24 09:57:14 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...
PRICIN~1			2558-03-24 09:57:32 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...
progress			2558-03-24 09:54:54 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...
proposal			2558-03-24 09:55:18 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...
TECHNI~1			2558-03-24 09:56:22 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...



Name	S	C	Modified Time	Access Time	Location
..			0000-00-00 00:00:00	0000-00-00 00:00:00	
[current folder]			2558-03-24 09:57:14 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...
winter_storm.amr			2558-01-23 16:47:10 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...
winter_whether_advisory.zip			2557-12-16 12:10:26 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph...

According to accessed time these are directories that were traversed in RM#2

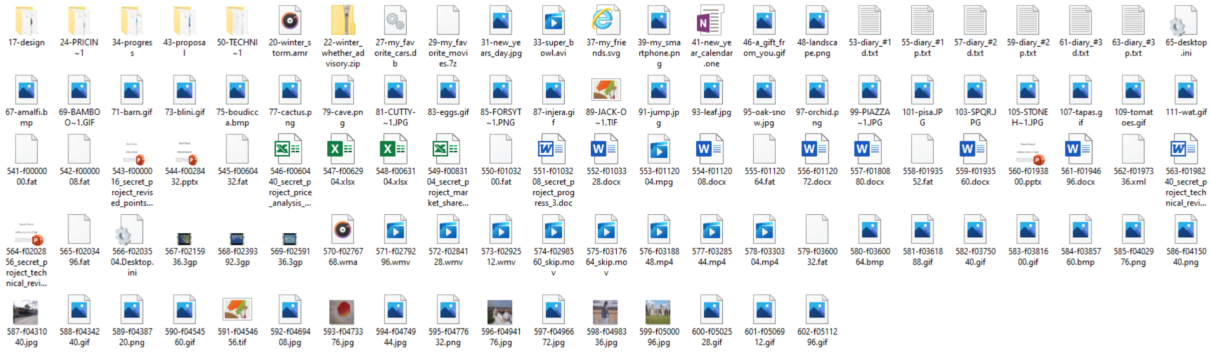
2. List all files that were opened in 'RM#2’.



Name	S	C	Modified Time	▽ Access Time	Location
design			2558-03-24 09:57:14 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
[current folder]			2558-03-24 09:57:14 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
winter_storm.amr			2558-01-23 16:47:10 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
winter_whether_advisory.zip			2557-12-16 12:10:26 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
PRICIN~1			2558-03-24 09:57:32 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
[current folder]			2558-03-24 09:57:32 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
my_favorite_cars.db			2558-01-16 15:10:24 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
my_favorite_movies.7z			2558-01-08 17:08:24 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
new_years_day.jpg			2557-12-01 14:50:26 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
super_bowl.avi			2557-12-02 13:28:58 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
progress			2558-03-24 09:54:54 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
[current folder]			2558-03-24 09:54:54 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
my_friends.svg			2558-01-20 11:13:44 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
my_smartphone.png			2558-01-05 11:57:22 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
new_year_calendar.one			2558-01-12 14:23:42 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
proposal			2558-03-24 09:55:18 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
[current folder]			2558-03-24 09:55:18 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
a_gift_from_you.gif			2557-12-18 17:50:58 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
landscape.png			2557-12-19 15:53:46 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
TECHNI~1			2558-03-24 09:56:22 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
[current folder]			2558-03-24 09:56:22 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
diary_#1d.txt			2558-01-05 17:01:08 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
diary_#1p.txt			2558-01-05 15:15:08 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
diary_#2d.txt			2558-01-12 17:25:40 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
diary_#2p.txt			2558-01-12 15:20:26 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
diary_#3d.txt			2558-01-20 16:05:00 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
diary_#3p.txt			2558-01-20 14:18:06 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..
desktop.ini			2558-03-24 15:51:48 ICT	2558-03-24 00:00:00 ICT	/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/$Orph..

Beside [current folder] and other folder such as “design” these may be the files that were opened in ‘RM#2’ according to accessed time.

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



17-design 24-PRICIN~1 34-progress 43-proposal 50-TECHNI~1 20-winter_storm.amr 22-winter_whether_advisory.zip 27-my_favorite_cars.db 29-my_favorite_movies.7z 31-new_years_day.jpg 33-super_bowl.avi 37-my_friends.svg 39-my_smartphone.png 41-new_year_calendar.one 46-a_gift_from_you.gif 48-landscape.png 53-diary_#1d.txt 55-diary_#1p.txt 57-diary_#2d.txt 59-diary_#2p.txt 61-diary_#3d.txt 63-diary_#3p.txt 65-desktop.ini

67-amalfi.bmp 69-BAMBOO~1.GIF 71-barn.gif 73-blini.gif 75-boudicca.bmp 77-cactus.png 79-cave.png 81-CUTTY-~1.JPG 83-eggs.gif 85-FORSYT~1.PNG 87-injera.gif 89-JACK-O~1.TIF 91-jump.jpg 93-leaf.jpg 95-oak-snow.jpg 97-orchid.png 99-PIAZZA~1.JPG 101-pisa.JPG 103-SPQR.JPG 105-STONEH~1.JPG 107-tapas.gif 109-tomatoes.gif 111-wat.gif

541-f0000000.fat 542-f0000008.fat 543-f0000016_secret_project_revised_points... 544-f0028432.pptx 545-f0060432.fat 546-f0060440_secret_project_price_analysis_... 547-f0062904.xlsx 548-f0063104.xlsx 549-f0083104_secret_project_market_share... 550-f0103200.fat 551-f0103208_secret_project_progress_3.doc 552-f0103328.docx 553-f0112004.mpg 554-f0112008.docx 555-f0112064.fat 556-f0112072.docx 557-f0180880.docx 558-f0193552.fat 559-f0193560.docx 560-f0193800.pptx 561-f0194696.docx 562-f0197336.xml 563-f0198240_secret_project_technical_revi...

564-f0202856_secret_project_technical_revi... 565-f0203496.fat 566-f0203504.Desktop.ini 567-f0215936.3gp 568-f0239392.3gp 569-f0259136.3gp 570-f0276768.wma 571-f0279296.wmv 572-f0284128.wmv 573-f0292512.wmv 574-f0298560_skip.mov 575-f0317664_skip.mov 576-f0318848.mp4 577-f0328544.mp4 578-f0330304.mp4 579-f0360032.fat 580-f0360064.bmp 581-f0361888.gif 582-f0375040.gif 583-f0381600.gif 584-f0385760.bmp 585-f0402976.png 586-f0415040.png

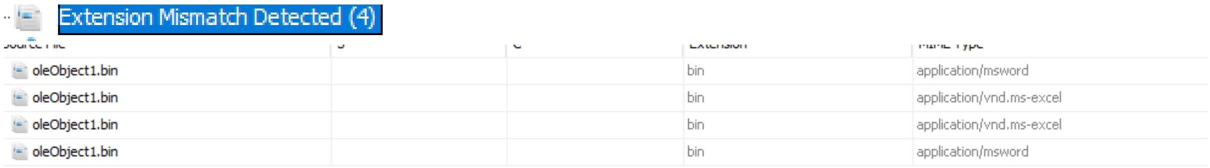
587-f0431040.jpg 588-f0434240.gif 589-f0438720.png 590-f0454560.gif 591-f0454656.tif 592-f0469408.jpg 593-f0473376.jpg 594-f0474944.jpg 595-f0477632.png 596-f0494176.jpg 597-f0496672.jpg 598-f0498336.jpg 599-f0500096.jpg 600-f0502528.gif 601-f0506912.gif 602-f0511296.gif

These are recovered files

4. What actions were performed for anti-forensics on USB drive ‘RM#2’? [Hint: this can be inferred from the results of the above question]

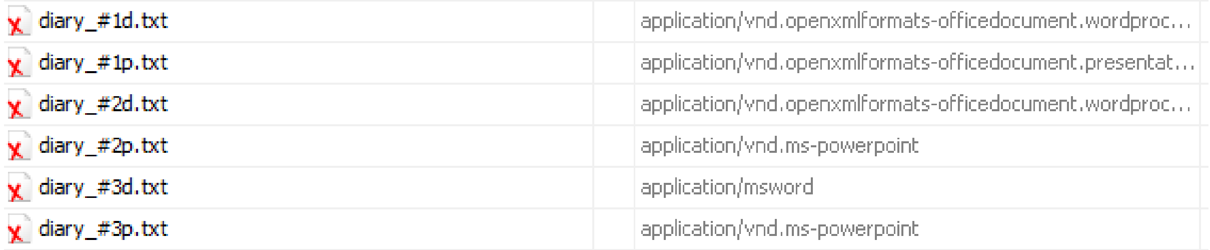
1. Format removable drive

2. Change file type / name



Extension Mismatch Detected (4)

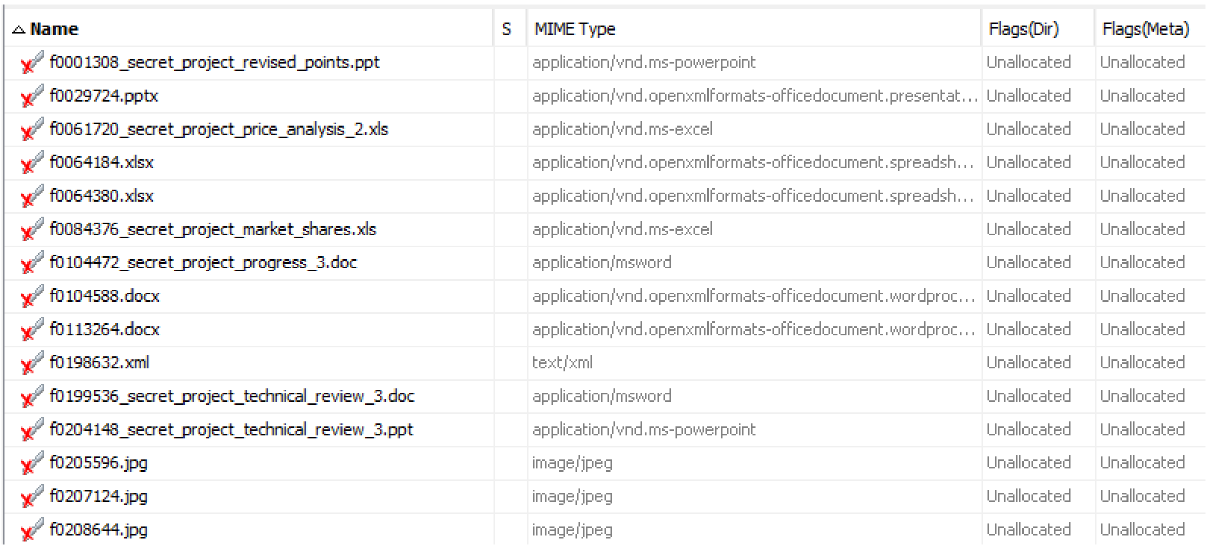
oleObject1.bin			bin	application/msword
oleObject1.bin			bin	application/vnd.ms-excel
oleObject1.bin			bin	application/vnd.ms-excel
oleObject1.bin			bin	application/msword



diary_#1d.txt	application/vnd.openxmlformats-officedocument.wordproc...
diary_#1p.txt	application/vnd.openxmlformats-officedocument.presentat...
diary_#2d.txt	application/vnd.openxmlformats-officedocument.wordproc...
diary_#2p.txt	application/vnd.ms-powerpoint
diary_#3d.txt	application/msword
diary_#3p.txt	application/vnd.ms-powerpoint

Examine media #3.

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



Name	S	MIME Type	Flags(Dir)	Flags(Meta)
f0001308_secret_project_revised_points.ppt		application/vnd.ms-powerpoint	Unallocated	Unallocated
f0029724.pptx		application/vnd.openxmlformats-officedocument.presentat...	Unallocated	Unallocated
f0061720_secret_project_price_analysis_2.xls		application/vnd.ms-excel	Unallocated	Unallocated
f0064184.xlsx		application/vnd.openxmlformats-officedocument.spreadsh...	Unallocated	Unallocated
f0064380.xlsx		application/vnd.openxmlformats-officedocument.spreadsh...	Unallocated	Unallocated
f0084376_secret_project_market_shares.xls		application/vnd.ms-excel	Unallocated	Unallocated
f0104472_secret_project_progress_3.doc		application/msword	Unallocated	Unallocated
f0104588.docx		application/vnd.openxmlformats-officedocument.wordproc...	Unallocated	Unallocated
f0113264.docx		application/vnd.openxmlformats-officedocument.wordproc...	Unallocated	Unallocated
f0198632.xml		text/xml	Unallocated	Unallocated
f0199536_secret_project_technical_review_3.doc		application/msword	Unallocated	Unallocated
f0204148_secret_project_technical_review_3.ppt		application/vnd.ms-powerpoint	Unallocated	Unallocated
f0205596.jpg		image/jpeg	Unallocated	Unallocated
f0207124.jpg		image/jpeg	Unallocated	Unallocated
f0208644.jpg		image/jpeg	Unallocated	Unallocated

By carving unallocated space between partition the hidden files that stored there are retrieved

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

   - format
   - renaming
   - hide files