

Activity 10 - 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.

Even though the files have been deleted from the file system and become unallocated, the actual data is still there and will not disappear until overwritten, thus items can still be found and opened.

2. How many objects can you find?

14 objects, all deleted files.

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.

All the objects are as follows:

Listing												
All												
Table Thumbnail Summary												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	
✖ f0023981_yword60.zip			1	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	Unallocated	unknown	
✖ f0023957.ppt			1	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	Unallocated	unknown	
✖ f0021929.wmv			1	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	Unallocated	unknown	
✖ f0020853_moov.mov			1	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	Unallocated	unknown	
✖ f0020841.gif			1	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	Unallocated	unknown	
✖ f0020645.jpg			1	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	Unallocated	unknown	
✖ f0019777.jpg			1	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	Unallocated	unknown	
✖ f0019717.jpg			1	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	Unallocated	unknown	
✖ f0019477.pdf			1	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	Unallocated	unknown	
✖ f0016741_Prudent_Engineering_Practice_for_Cryptographic_Protocols.pdf			1	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	Unallocated	unknown	
✖ f0016693.xls			1	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	Unallocated	unknown	
✖ f0016021.wav			1	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	Unallocated	unknown	
✖ f0000321.wmv			1	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	Unallocated	unknown	
✖ f0000281_Nick_is_a_pretty_man_with_a_2003_document.doc			1	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	Unallocated	unknown	

All the content is accessible, but are all already deleted, as file name and metadata are unallocated for all of the files.

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?

We need to format the disk by writing a single pass of zeros to the drive. The time varies, but according to <https://www.techwalla.com/articles/how-long-does-it-take-to-wipe-your-hard-drive> 20GB takes 1 hour, so 1TB would take 50 hours.

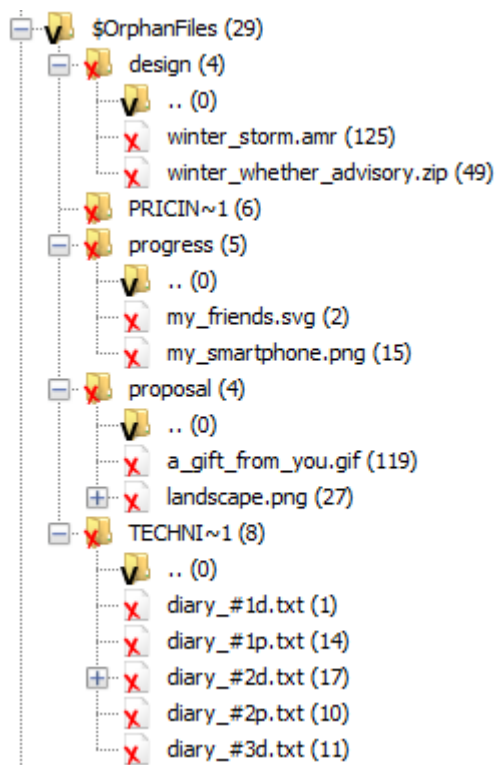
5. Will file carving be able to recover deleted files on an SSD? Why or why not?

It is nearly impossible on a modern SSD that supports the TRIM command. With TRIM, deleted files are removed immediately and can't be recovered. However it may be possible to disable TRIM by some method.

Part 2: Investigation

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

All of the orphaned directories.



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







































All the files in these images (they were inside the orphaned directories).

2015-03-23 00:00:00 to 2015-03-24 00:00:01

46 Results

Table Thumbnail Summary

Save Table as CSV

Icon	Date/Time	Description	Event Type
	2015-03-23 00:00:00	/\$OrphanFiles/STONEH~1.JPG	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/TECHNI~1/diary_#3p.txt	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/design	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/tapas.gif	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/desktop.ini	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/design/winter_storm.amr	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/tomatoes.gif	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/amalfi.bmp	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/design/winter_weather_advisory.zip	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/wat.gif	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/BAMBOO~1.GIF	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/PRICIN~1	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/barn.gif	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/PRICIN~1/my_favorite_cars.db	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/blini.gif	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/PRICIN~1/my_favorite_movies.7z	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/boudicca.bmp	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/PRICIN~1/new_years_day.jpg	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/cactus.png	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/PRICIN~1/super_bowl.avi	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/cave.png	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/progress	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/CUTTY~1.JPG	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/progress/my_friends.svg	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/eggs.gif	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/progress/my_smartphone.png	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/FORSYT~1.PNG	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/progress/new_year_calendar.one	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/injera.gif	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/proposal	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/JACK-O~1.TIF	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/proposal/a_gift_from_you.gif	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/jump.jpg	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/proposal/landscape.png	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/leaf.jpg	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/TECHNI~1	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/oak-snow.jpg	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/TECHNI~1/diary_#1d.txt	File Accessed

	2015-03-23 00:00:00	/\$OrphanFiles/orchid.png	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/TECHNI~1/diary_#1p.txt	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/PIAZZA~1.JPG	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/TECHNI~1/diary_#2d.txt	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/pisa.JPG	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/TECHNI~1/diary_#2p.txt	File Accessed
	2015-03-23 00:00:00	/\$OrphanFiles/SPQR.JPG	File Accessed
	2015-03-24 00:00:00	/\$OrphanFiles/TECHNI~1/diary_#3d.txt	File Accessed

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

We were able to recover most files from the directories in question 1, but the files were unable to be opened in image viewers even though they were image formats such as `.gif` or `.jpeg`.

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]

- The file extensions and file names of the 'secret project' files were changed to various formats such as `.gif`, `.jpeg`, or `.one`.
- The files were kept in various separate folders with different names.
- All the suspicious files were orphan files, likely because they were shared through a cloud storage and the storage was deleted.
- Some files were modified by writing repeating strings into the the file, and hiding some data between the repeating strings.

Timeline - Editor

Timeline X

2013-05-07 14:48:44 to 2015-03-24 15:51:49

123 Results

Table Thumbnail Summary

Save Table as CSV

Icon	Date/Time	Description	Event Type
	2013-05-07 15:09:52	/OrphanFiles/bins.gf	File Modified
	2013-05-07 14:48:44	/OrphanFiles/boudca.bmp	File Modified
	2013-05-07 15:11:10	/OrphanFiles/apas.gf	File Modified
	2013-05-07 15:10:20	/OrphanFiles/njira.gf	File Modified
	2013-05-07 15:10:50	/OrphanFiles/tomatoes.gf	File Modified
	2013-05-07 15:19:42	/OrphanFiles/amafl.bmp	File Modified
	2013-05-07 15:37:56	/OrphanFiles/JACK-O-1.TIF	File Modified
	2013-05-07 15:12:28	/OrphanFiles/wat.gf	File Modified
	2014-12-01 14:50:26	/OrphanFiles/PRJCDN-1/new_years_day.jpg	File Modified
	2014-12-02 13:28:58	/OrphanFiles/PRJCDN-1/super_bowl.avi	File Modified
	2014-12-16 12:10:26	/OrphanFiles/design/winter_weather_advisory.zip	File Modified
	2014-12-18 17:50:58	/OrphanFiles/proposals/gift_from_you.gf	File Modified
	2014-12-19 15:53:46	/OrphanFiles/proposals/landscape.png	File Modified
	2015-01-16 15:10:24	/OrphanFiles/PRJCDN-1/my_favorite_cars.db	File Modified
	2015-01-20 16:05:00	/OrphanFiles/TECHN-1/dary_#3d.txt	File Modified
	2015-01-05 11:57:22	/OrphanFiles/progress/my_smartphone.png	File Modified
	2015-01-08 17:08:24	/OrphanFiles/PRJCDN-1/my_favorite_movies.7z	File Modified
	2015-01-20 14:18:06	/OrphanFiles/TECHN-1/dary_#3p.txt	File Modified
	2015-01-05 17:01:08	/OrphanFiles/TECHN-1/dary_#1d.txt	File Modified
	2015-01-12 14:23:42	/OrphanFiles/progress/new_year_calendar.one	File Modified
	2015-01-05 15:15:08	/OrphanFiles/TECHN-1/dary_#1p.txt	File Modified
	2015-01-23 16:47:10	/OrphanFiles/design/winter_storm.amr	File Modified
	2015-01-12 17:25:40	/OrphanFiles/TECHN-1/dary_#2d.txt	File Modified
	2015-01-12 15:20:26	/OrphanFiles/TECHN-1/dary_#2p.txt	File Modified
	2015-01-20 11:13:44	/OrphanFiles/progress/my_friends.svg	File Modified
	2015-03-24 09:59:26	/OrphanFiles/design	File Created
	2015-03-24 00:00:00	/OrphanFiles/design	File Accessed
	2015-03-24 09:57:14	/OrphanFiles/design	File Modified
	2015-03-24 09:59:27	/OrphanFiles/design/winter_storm.amr	File Created
	2015-03-24 00:00:00	/OrphanFiles/design/winter_storm.amr	File Accessed
	2015-03-24 09:59:37	/OrphanFiles/design/winter_weather_advisory.zip	File Created
	2015-03-24 00:00:00	/OrphanFiles/design/winter_weather_advisory.zip	File Accessed
	2015-03-24 09:59:39	/OrphanFiles/PRJCDN-1	File Created
	2015-03-24 00:00:00	/OrphanFiles/PRJCDN-1	File Accessed
	2015-03-24 09:57:32	/OrphanFiles/PRJCDN-1	File Modified
	2015-03-24 09:59:39	/OrphanFiles/PRJCDN-1/my_favorite_cars.db	File Created
	2015-03-24 00:00:00	/OrphanFiles/PRJCDN-1/my_favorite_cars.db	File Accessed
	2015-03-24 09:59:39	/OrphanFiles/PRJCDN-1/my_favorite_movies.7z	File Created

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 14 of 17 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

Timeline - Editor

Timeline X

2013-05-07 14:48:44 to 2015-03-24 15:51:49

123 Results

Table Thumbnail Summary

Save Table as CSV

Icon	Date/Time	Description	Event Type
	2013-05-07 15:09:52	/OrphanFiles/bins.gf	File Modified
	2013-05-07 14:48:44	/OrphanFiles/boudca.bmp	File Modified
	2013-05-07 15:11:10	/OrphanFiles/apas.gf	File Modified
	2013-05-07 15:10:20	/OrphanFiles/njira.gf	File Modified
	2013-05-07 15:10:50	/OrphanFiles/tomatoes.gf	File Modified
	2013-05-07 15:19:42	/OrphanFiles/amafl.bmp	File Modified
	2013-05-07 15:37:56	/OrphanFiles/JACK-O-1.TIF	File Modified
	2013-05-07 15:12:28	/OrphanFiles/wat.gf	File Modified
	2014-12-01 14:50:26	/OrphanFiles/PRJCDN-1/new_years_day.jpg	File Modified
	2014-12-02 13:28:58	/OrphanFiles/PRJCDN-1/super_bowl.avi	File Modified
	2014-12-16 12:10:26	/OrphanFiles/design/winter_weather_advisory.zip	File Modified
	2014-12-18 17:50:58	/OrphanFiles/proposals/gift_from_you.gf	File Modified
	2014-12-19 15:53:46	/OrphanFiles/proposals/landscape.png	File Modified
	2015-01-16 15:10:24	/OrphanFiles/PRJCDN-1/my_favorite_cars.db	File Modified
	2015-01-20 16:05:00	/OrphanFiles/TECHN-1/dary_#3d.txt	File Modified
	2015-01-05 11:57:22	/OrphanFiles/progress/my_smartphone.png	File Modified
	2015-01-08 17:08:24	/OrphanFiles/PRJCDN-1/my_favorite_movies.7z	File Modified
	2015-01-20 14:18:06	/OrphanFiles/TECHN-1/dary_#3p.txt	File Modified
	2015-01-05 17:01:08	/OrphanFiles/TECHN-1/dary_#1d.txt	File Modified
	2015-01-12 14:23:42	/OrphanFiles/progress/new_year_calendar.one	File Modified
	2015-01-05 15:15:08	/OrphanFiles/TECHN-1/dary_#1p.txt	File Modified
	2015-01-23 16:47:10	/OrphanFiles/design/winter_storm.amr	File Modified
	2015-01-12 17:25:40	/OrphanFiles/TECHN-1/dary_#2d.txt	File Modified
	2015-01-12 15:20:26	/OrphanFiles/TECHN-1/dary_#2p.txt	File Modified
	2015-01-20 11:13:44	/OrphanFiles/progress/my_friends.svg	File Modified
	2015-03-24 09:59:26	/OrphanFiles/design	File Created
	2015-03-24 00:00:00	/OrphanFiles/design	File Accessed
	2015-03-24 09:57:14	/OrphanFiles/design	File Modified
	2015-03-24 09:59:27	/OrphanFiles/design/winter_storm.amr	File Created
	2015-03-24 00:00:00	/OrphanFiles/design/winter_storm.amr	File Accessed
	2015-03-24 09:59:37	/OrphanFiles/design/winter_weather_advisory.zip	File Created
	2015-03-24 00:00:00	/OrphanFiles/design/winter_weather_advisory.zip	File Accessed
	2015-03-24 09:59:39	/OrphanFiles/PRJCDN-1	File Created
	2015-03-24 00:00:00	/OrphanFiles/PRJCDN-1	File Accessed
	2015-03-24 09:57:32	/OrphanFiles/PRJCDN-1	File Modified
	2015-03-24 09:59:39	/OrphanFiles/PRJCDN-1/my_favorite_cars.db	File Created
	2015-03-24 00:00:00	/OrphanFiles/PRJCDN-1/my_favorite_cars.db	File Accessed
	2015-03-24 09:59:39	/OrphanFiles/PRJCDN-1/my_favorite_movies.7z	File Created

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 15 of 17 Page

Matches on page: - of - Match

100%

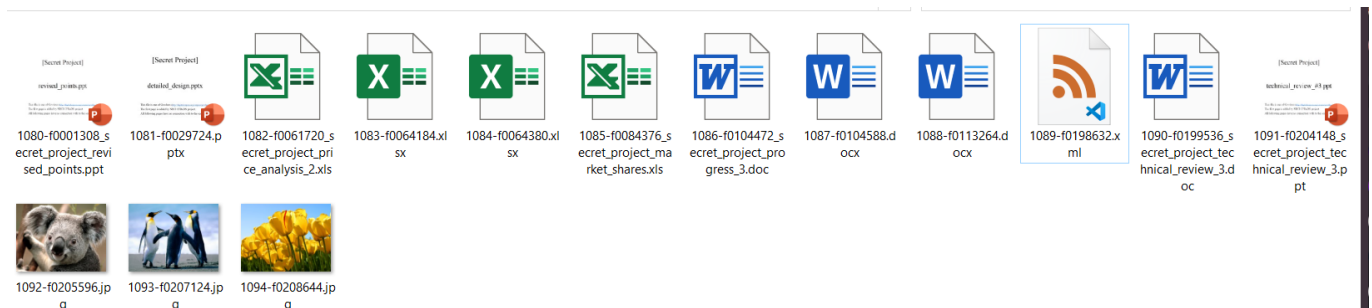
Reset

Text Source: File Text

year the project first entered the budget system.
The 24 FMC E-Gov initiatives end in a code of 24 reflecting cross-government participation. <
Comments:
Type of Projects:
01 - means a major project as defined in OMB Circular A-11 and the agencies' capital planning processes.
02 - Small and Other projects as defined by the agencies. <
Comments:
Total Investments reflect the total of all development and steady state funding for a particular project. Please note, there are rounding errors due to reporting in millions, zeros indicate that the amount is below the million mark. Also, d
evelopment and steady state do not add up to total investments as many small projects do not breakout the development and steady state funding. <
Comments:
This category represents any portion of the investment that is identified as development, modernization, or enhancement efforts. <
Comments:
This category represents the portion of the investments that is identified as steady state or operate and maintain costs. <
William McVay
William McVay
William McVay
William McVay
William McVay
William McVay >
dg
MSPT
Microsoft Office Document Inag
Letter
width
ffffmmmmmmmmmmmm
zzzzzzzzzzzzzzzzzz
oooooooooooooooooooo
oooooooooooooooooooo
oooooooooooooooooooo
ffff
56~
[5~
ffff~
H&B~
~#B~
z&B~
~5B~
~<5B~
RUB~
z<UB~
A 9B~
+~+~+~
fffffA&B~
z&+~
z&B~
fffff~
fffff~
ffff
C~>B~
ffff
z&B~
Byygrwqrrrr
Byygrwqrrrr
Byygrwqrrrr
Byygrwqrrrr
Byygrwqrrrr
Byygrwqrrrr

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

Multiple Powerpoint, Excel, and Word files about the 'secret project'. After recovery, it was possible to open all of them.



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

- The files were deleted from storage.