

Activity X: Computer Forensics

By Saenyakorn Siangsanoh 6232035721 and Poravee Binhayearason 6230314421

สามารถดู Resource เต็ม ๆ ได้ที่ [2110413-COMP-SECURITY Activity 10](#)

Table of Contents

- [Part I File Carving](#)
 - [1](#)
 - [Answer](#)
 - [2](#)
 - [Answer](#)
 - [3](#)
 - [Answer](#)
 - [4](#)
 - [Answer](#)
 - [5](#)
 - [Answer](#)
- [Part II Investigation](#)
 - [1](#)
 - [Answer](#)
 - [2](#)
 - [Answer](#)
 - [3](#)
 - [Answer](#)
 - [4](#)
 - [Answer](#)
 - [5](#)
 - [Answer](#)
 - [6](#)
 - [Answer](#)

Part I 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.

Answer

เพราะหลาย ๆ file ที่ถูกลบ ถูกลบด้วยวิธี Quick format ซึ่งมันจะทำการลบไฟล์ด้วยวิธี mark ว่าพื้นที่ตรงนั้นสามารถเขียนทับได้ แต่ไม่มีการ write ให้ที่ตรงนั้นเป็นค่าว่าง ดังนั้นเราจึงยังสามารถดูไฟล์ที่ถูกลบได้

2

How many objects can you find?

Answer

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.

Answer

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0000281_Nick_is_a_pretty_man_with_a_2003_document.doc			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	19968	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0000321.wmv			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	8037267	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0016021.wav			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	21888	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0016693.xls			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	23040	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0016741_Prudent_Engineering_Practice_for_Cryptographic_Protocols.pdf			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	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0019477.pdf			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	122434	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0019717.jpg			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	29885	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0019777.jpg			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	444314	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0020645.jpg			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	99298	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0020841.gif			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	5498	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0020853_moov.mov			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	550653	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0021929.wmv			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	1036994	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0023957.ppt			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	11264	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car
f0023981_vword50.zip			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	78899	Unallocated	Unallocated	unknown	/img_forensics-p2.dd/\$Car

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?

Answer

Overwrite hard disk อย่างน้อย 1-3 ครั้งเพื่อให้มั่นใจว่าทุก bad sector ถูกเขียนทับแล้ว โดยเราสามารถคำนวณเวลาที่ทำได้โดยการ สมมติว่า hard disk 1TB และ write speed ของ hard disk คือ 100MB/s ดังนั้นใช้เวลา $10,000s = 2.78$ ชั่วโมง ต่อการ write 1 ครั้ง

5

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

Answer

ไม่ได้ ถ้าหากว่า data ที่โดน TRIM ไปแล้วยังไม่ถูกเขียนทับด้วยข้อมูลอื่น

Part II Investigation

1

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

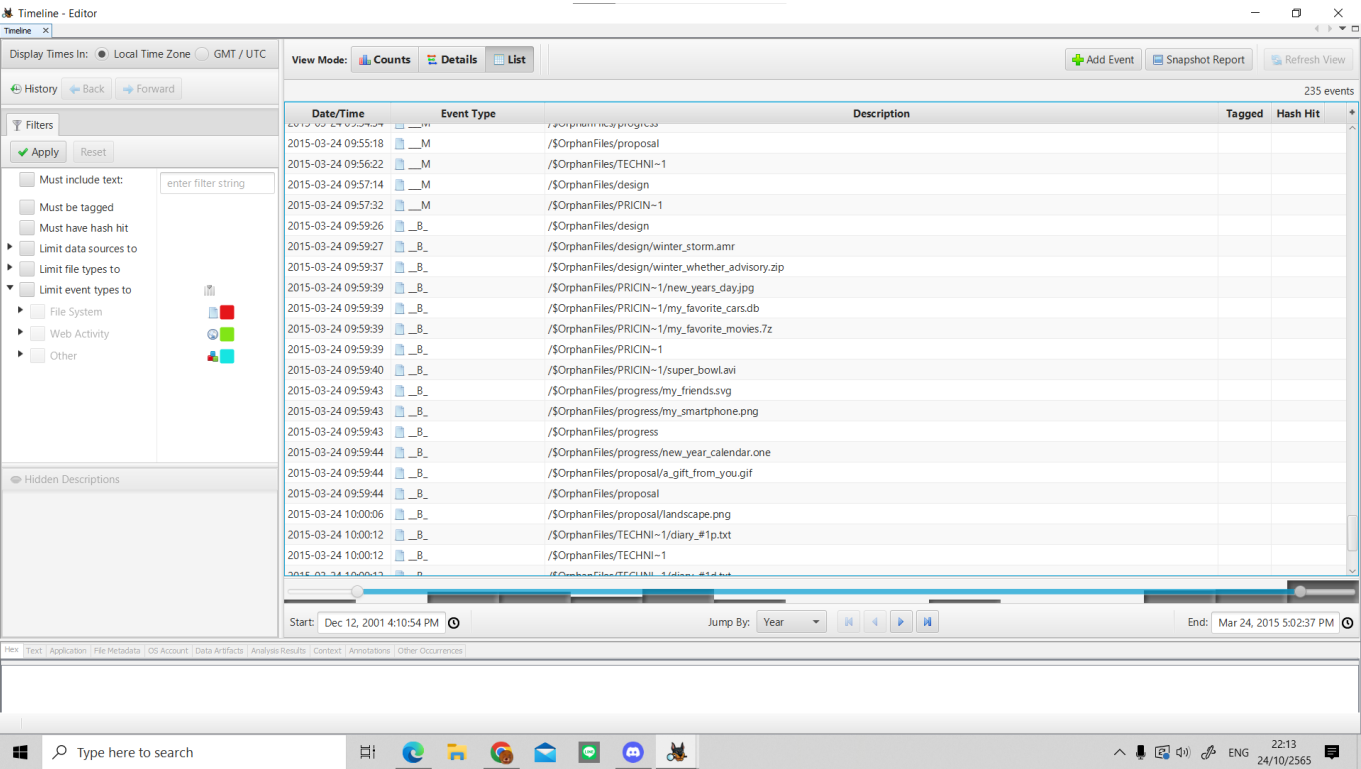
Answer



2

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

Answer



3

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

Answer

ทุกไฟล์ใน CarvedFiles และ OrphanFiles folder

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]

Answer

Listing

/img_cfreds_2015_data_leakage_rm#2.dd/vol_vol2/\$OrphanFiles/PRICIN~1

Table Thumbnail Summary

6 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash	SHA-2
..				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Allocated	unknown		
[current folder]				2558-03-24 09:57:32 ICT	0000-00-00 00:00:00	2558-03-24 00:00:00 ICT	2558-03-24 09:59:39 ICT	4096	Unallocated	Unallocated	unknown		
my_favorite_cars.db				2558-01-16 15:10:24 ICT	0000-00-00 00:00:00	2558-03-24 00:00:00 ICT	2558-03-24 09:59:39 ICT	1260544	Unallocated	Unallocated	unknown	a23c3ed3cf482a3d5c420f6ff4fea6f6	c3a276
my_favorite_movies.7z				2558-01-08 17:08:24 ICT	0000-00-00 00:00:00	2558-03-24 00:00:00 ICT	2558-03-24 09:59:39 ICT	100078	Unallocated	Unallocated	unknown	975d98575f92d2e466ecb96d39701fc8	a21c97
new_years_day.jpg				2557-12-01 14:50:26 ICT	0000-00-00 00:00:00	2558-03-24 00:00:00 ICT	2558-03-24 09:59:39 ICT	10237535	Unallocated	Unallocated	unknown	0329d88f08a8cb2c8057a8fa9418f9f3	616188
super_bowl.avi				2557-12-02 13:28:58 ICT	0000-00-00 00:00:00	2558-03-24 00:00:00 ICT	2558-03-24 09:59:40 ICT	10289152	Unallocated	Unallocated	unknown	2ebbbb59b8019a94c7416d9acbaad658	1ff925

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

Strings Indexed Text Translation

Page: 1 of 93 Page Matches on page: - of - Match 100% Reset Text Source: File Text

NIST

[Secret Project]

market_shares.xls

This file is one of Govdocs (<http://digital.corpora.org/corpora/govdocs>)

The first sheet is added by NIST CFReDS project.

All following sheets have no connection with the scenario.

Please read first

This document is a companion to Chapter 9 of the Analytical Perspectives volume of this budget, and provides the Information Technology (IT) portfolios discussed in the Budget. For additional guidance about the formulation of the Information Technology and E-gov Exhibit 53s for the FY2009 budget, please go to:

http://www.whitehouse.gov/omb/circulars/a11/current_year/s53.pdf

For additional guidance about the Planning, Budgeting, Acquisition of Capital Assets, Exhibit 300s for the FY2009 budget, please go to:

http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf

The document consists of Microsoft Excel Worksheets:

Summary Worksheet: This worksheet provides an overall summary of IT spending, by agency or department, for FY2007, FY2008, and FY2009. Each agency name is hyperlinked to the agency's worksheet of this report providing details for the agency.

IT Investment Details Worksheet: This worksheet provides agency IT investment details in the categories of 1) investments by mission area, 2) office automation and infrastructure investments, 3) enterprise architecture and planning investments, 4) grants management investments, 5) Grants to State and Local, and 6) National Security Systems. The breakout of modernization funds versus steady state operations are displayed if reported by the agencies. The report is in millions of dollars and some small/other investments do not breakout the modernization from the steady state so they may appear to be errors in addition. There are comment fields for each key heading describing the elements of the report.

Agency Worksheets: These worksheets provide each agency IT investment details in the categories of 1) investments by mission area, 2) office automation and infrastructure investments, 3) enterprise architecture and planning investments, 4) grants management investments, 5) Grants to State and Local, and 6) National Security Systems. The breakout of modernization funds versus steady state operations are displayed if reported by the agencies. The report is in millions of dollars and some small/other investments do not breakout the modernization from the steady state so they may appear to be errors in addition. There are comment fields for each key heading describing the elements of the report.

How Ex 53 is coded Worksheet: This worksheet provides a summary of the information provided for in Circular A-11 Section 53.9.

If you have questions about this report please contact OMB Communications at 202-395-7254.

Additional References:

Federal Enterprise Architecture (FEA) Consolidated Reference Model (CRM) Version 2.3

http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf

FY09 FEA Reference Model Mapping Quick Guide (for the Exhibit 53 Primary FEA Mappings):

http://www.whitehouse.gov/omb/egov/documents/FY09_Ref_Model_Mapping_QuickGuide_July_2007.pdf

สังเกตว่าไฟล์ทั้งหลายมี Flag unallocated ซึ่งแปลว่ามีการพยายามลบข้อมูลด้วย Quick Format

5

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

Answer

ทุกไฟล์ใน CarvedFiles

Listing

/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles

15 Results

TableThumbnailSummary

Save Table as CSV

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			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0001308_secret_project_revised_points.ppt
f0029724.pptx			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0029724.pptx
f0061720_secret_project_price_analysis_2.xls			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0061720_secret_project_price_analysis_2.xls
f0064184.xlsx			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0064184.xlsx
f0064380.xlsx			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10237535	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0064380.xlsx
f0084376_secret_project_market_shares.xls			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0084376_secret_project_market_shares.xls
f0104472_secret_project_progress_3.doc			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	57344	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0104472_secret_project_progress_3.doc
f0104588.docx			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0104588.docx
f0113264.docx			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0113264.docx
f0198632.xml			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0198632.xml
f0199536_secret_project_technical_review_3.doc			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0199536_secret_project_technical_review_3.doc
f0204148_secret_project_technical_review_3.ppt			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0204148_secret_project_technical_review_3.ppt
f0205596.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	780831	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0205596.jpg
f0207124.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	777835	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0207124.jpg
f0208644.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	620888	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0208644.jpg

6

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

Answer

Listing

/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles

15 Results

TableThumbnailSummary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0104472_secret_project_progress_3.doc			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	57344	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0104472_secret_project_progress_3.doc
f0104588.docx			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0104588.docx
f0113264.docx			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0113264.docx
f0198632.xml			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0198632.xml
f0199536_secret_project_technical_review_3.doc			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0199536_secret_project_technical_review_3.doc
f0204148_secret_project_technical_review_3.ppt			2	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	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0204148_secret_project_technical_review_3.ppt
f0205596.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	780831	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0205596.jpg
f0207124.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	777835	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0207124.jpg
f0208644.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	620888	Unallocated	Unallocated	unknown	/img_cfreds_2015_data_leakage_rm#3_type2.dd/\$CarvedFiles/f0208644.jpg

สังเกตว่าไฟล์ทั้งหลายมี Flag unallocated ซึ่งแปลว่ามีการพยายาม format CD-R เพื่อซ่อนข้อมูลบางอย่าง