Part 1

Q1. 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 เมื่อผู้ใช้สั่งลบไฟล์ ระบบปฏิบัติการจะดำเนินการเพียงแค่ ลบหรือทำลายMetadata และรายงานว่าพื้นที่ดังกล่าวเป็นพื้นที่ที่ยังไม่ได้ใช้ ซึ่งการลบข้อมูลเมตาไม่ได้หมายความว่าระบบจะ ลบเนื้อหาไฟล์ (File Content) จริงๆ ที่อยู่ในเซกเตอร์ดิสก์ทันที ข้อมูลดิบของไฟล์ยังคงอยู่บนดิสก์ในพื้นที่ที่ถูกทำเครื่องหมายว่าเป็น "ว่าง" จนกว่าจะมีไฟล์ใหม่ถูกเขียนทับลงไป

Q2. How many objects can you find?

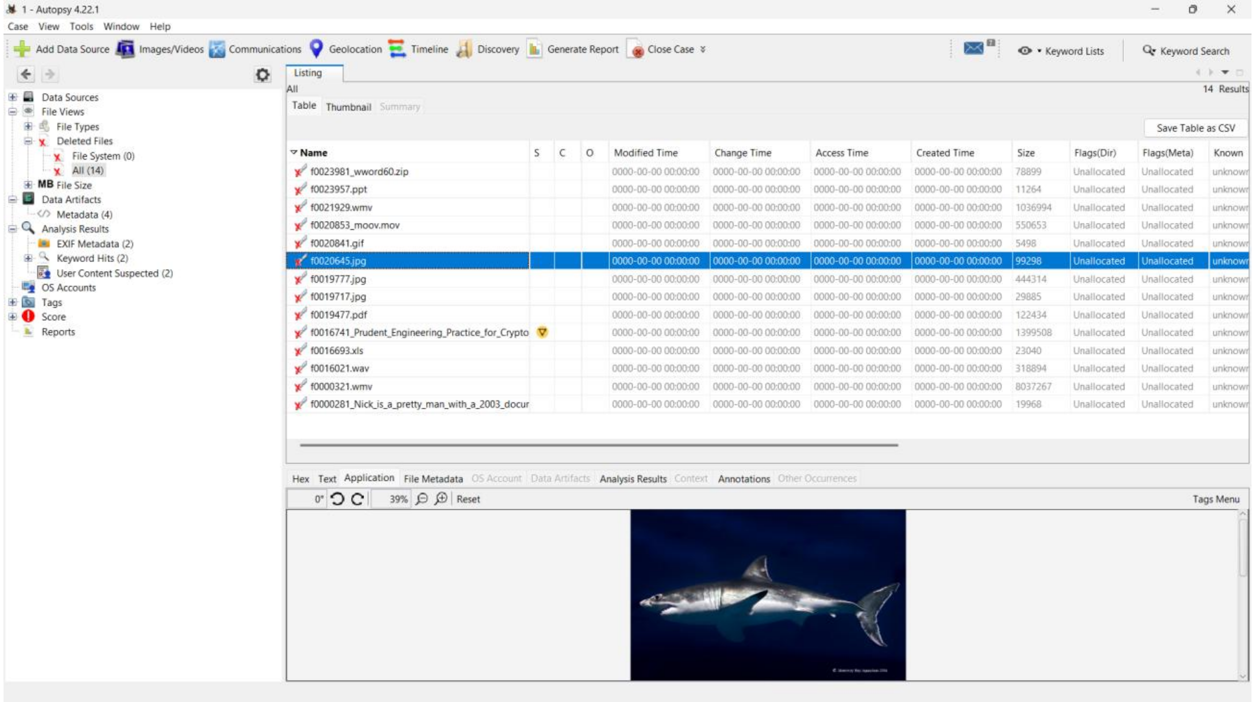
ANS 14

Q3. 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.

(open as logical file and read only text)

ANS can open only image and text file. Voice file cannot be opened



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
f0023981_wword60.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	Unallocated	unknown
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	Unallocated	unknown
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	Unallocated	unknown
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	Unallocated	unknown
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	Unallocated	unknown
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	Unallocated	unknown
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	Unallocated	unknown
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	Unallocated	unknown
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	Unallocated	unknown
f0016741_Prudent_Engineering_Practice_for_Crypto	▽			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				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				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				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_docur				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

Q4. 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?

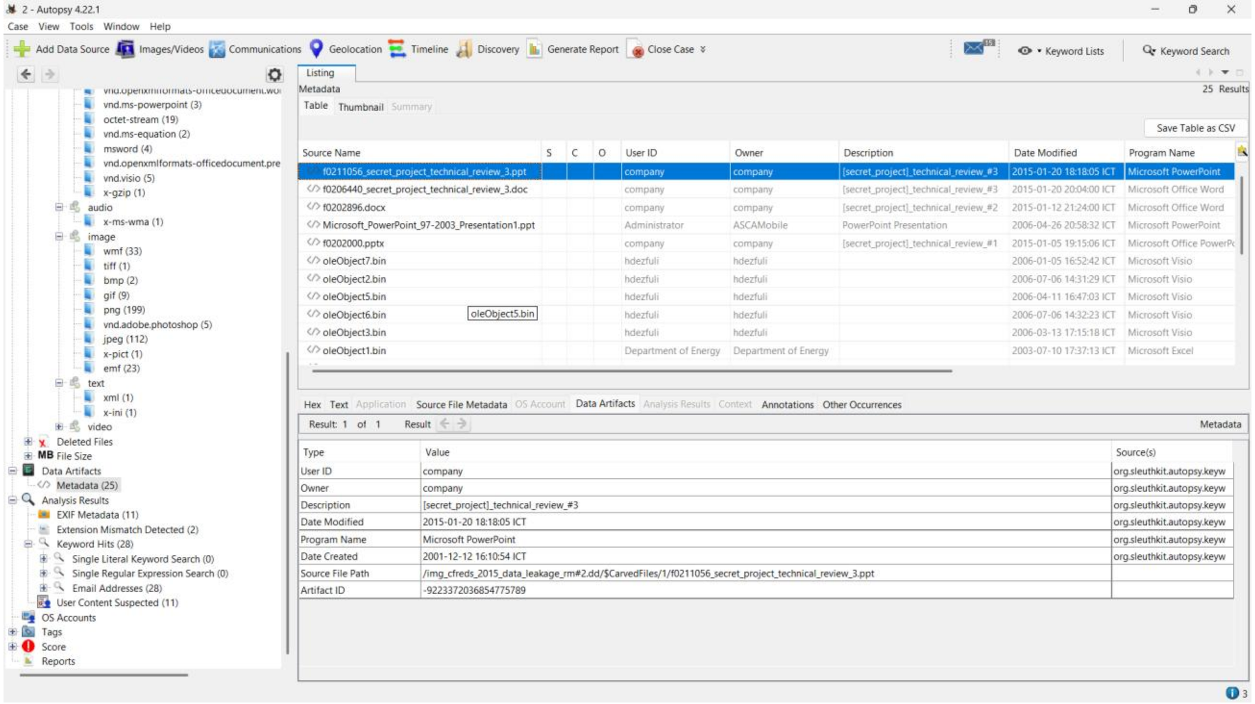
ANS การเขียนทับ อย่างน้อย7รอบ ประมาณ14ชั่งโมง หรือใช้แม่เหล็กแรงๆ ในไม่กี่วินาที

Q5. Will file carving be able to recover deleted files on an SSD? Why or why not?
ANS ไม่สามารถกู้คืนได้ หรือทำได้ยากมาก SSD ใช้คำสั่ง TRIM หรือ UNMAP ซึ่ง คอนโทรลเลอร์ SSD จะตอบสนองโดยการล้างข้อมูลจริง

Part2

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

ANS CarvedFiles



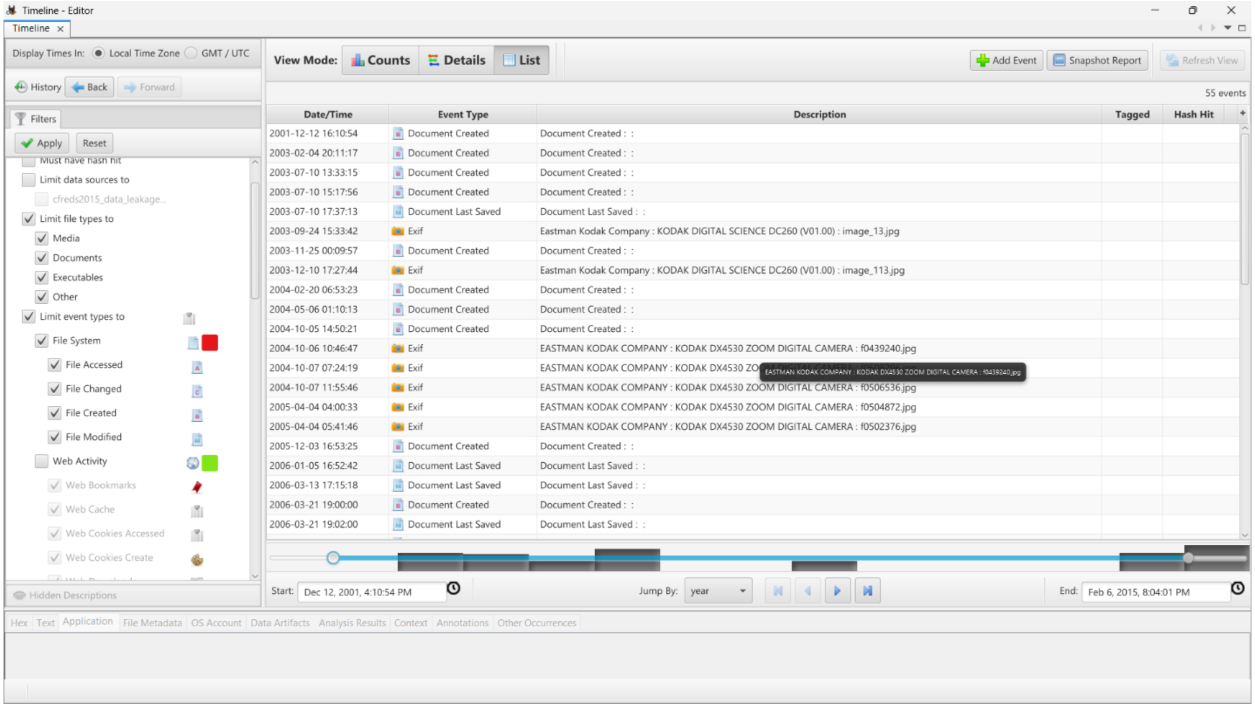
- vnd.openxmlformats-officedocument.wo
- vnd.ms-powerpoint (3)
- octet-stream (19)
- vnd.ms-equation (2)
- msword (4)
- vnd.openxmlformats-officedocument.pre
- vnd.visio (5)
- x-gzip (1)
- audio
  - x-ms-wma (1)
- image
  - wmf (33)
  - tiff (1)
  - bmp (2)
  - gif (9)
  - png (199)
  - vnd.adobe.photoshop (5)
  - jpeg (112)
  - x-pict (1)
  - emf (23)
- text
  - xml (1)
  - x-ini (1)
- video
- Deleted Files
- MB File Size
- Data Artifacts
  - Metadata (25)
- Analysis Results
  - EXIF Metadata (11)
  - Extension Mismatch Detected (2)
  - Keyword Hits (28)
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (28)
  - User Content Suspected (11)
- OS Accounts
- Tags
- Score
- Reports

Source Name	S	C	O	User ID	Owner	Description	Date Modified	Program Name
f0211056_secret_project_technical_review_3.ppt				company	company	[secret_project]_technical_review_#3	2015-01-20 18:18:05 ICT	Microsoft PowerPoint
f0206440_secret_project_technical_review_3.doc				company	company	[secret_project]_technical_review_#3	2015-01-20 20:04:00 ICT	Microsoft Office Word
f0202896.docx				company	company	[secret_project]_technical_review_#2	2015-01-12 21:24:00 ICT	Microsoft Office Word
Microsoft_PowerPoint_97-2003_Presentation1.ppt				Administrator	ASCAMobile	PowerPoint Presentation	2006-04-26 20:58:32 ICT	Microsoft PowerPoint
f0202000.pptx				company	company	[secret_project]_technical_review_#1	2015-01-05 19:15:06 ICT	Microsoft Office PowerPc
oleObject7.bin				hdezfuli	hdezfuli		2006-01-05 16:52:42 ICT	Microsoft Visio
oleObject2.bin				hdezfuli	hdezfuli		2006-07-06 14:31:29 ICT	Microsoft Visio
oleObject5.bin				hdezfuli	hdezfuli		2006-04-11 16:47:03 ICT	Microsoft Visio
oleObject6.bin oleObject5.bin				hdezfuli	hdezfuli		2006-07-06 14:32:23 ICT	Microsoft Visio
oleObject3.bin				hdezfuli	hdezfuli		2006-03-13 17:15:18 ICT	Microsoft Visio
oleObject1.bin				Department of Energy	Department of Energy		2003-07-10 17:37:13 ICT	Microsoft Excel

Type	Value	Source(s)
User ID	company	org.sleuthkit.autopsy.keyw
Owner	company	org.sleuthkit.autopsy.keyw
Description	[secret_project]_technical_review_#3	org.sleuthkit.autopsy.keyw
Date Modified	2015-01-20 18:18:05 ICT	org.sleuthkit.autopsy.keyw
Program Name	Microsoft PowerPoint	org.sleuthkit.autopsy.keyw
Date Created	2001-12-12 16:10:54 ICT	org.sleuthkit.autopsy.keyw
Source File Path	/img_cfreds_2015_data_leakage_rm#2.dd/$CarvedFiles/1/f0211056_secret_project_technical_review_3.ppt	
Artifact ID	-9223372036854775789	

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

ANS



Display Times In: ● Local Time Zone ○ GMT / UTC

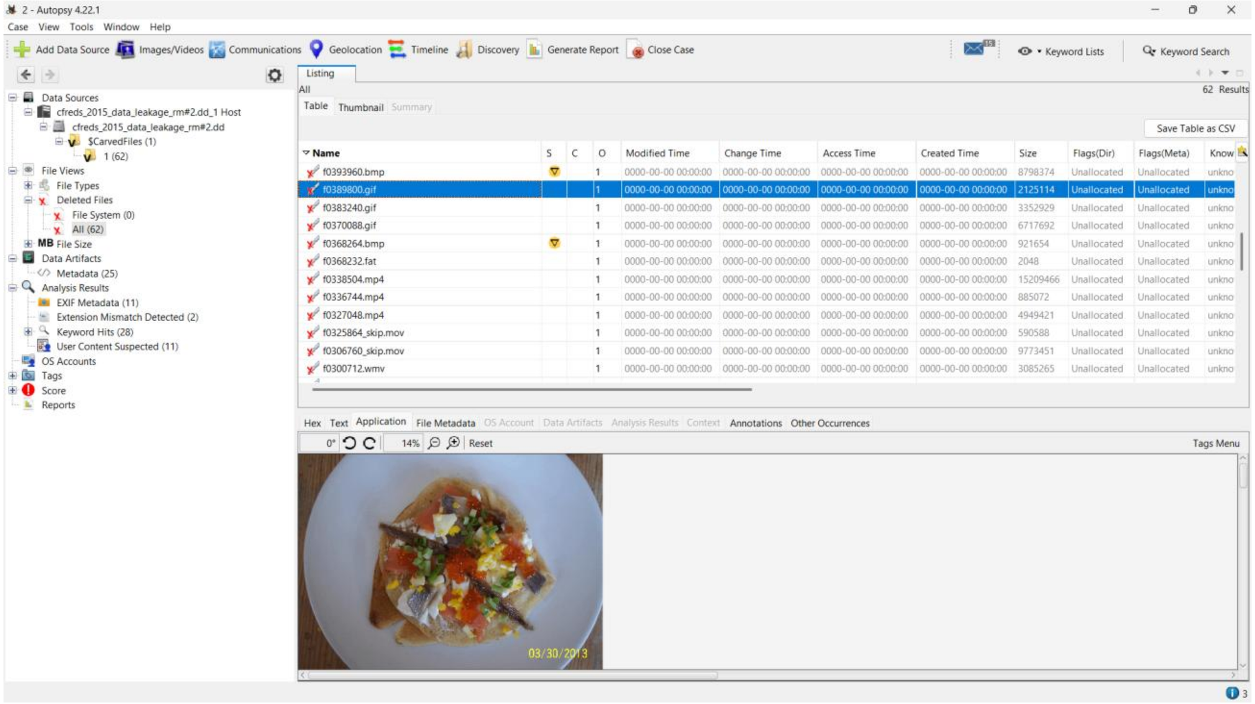
- □ Must have hash hit
- □ Limit data sources to
  - □ cfreds2015_data_leakage...
- ☑ Limit file types to
  - ☑ Media
  - ☑ Documents
  - ☑ Executables
  - ☑ Other
- ☑ Limit event types to
  - ☑ File System 🟥
    - ☑ File Accessed
    - ☑ File Changed
    - ☑ File Created
    - ☑ File Modified
  - □ Web Activity 🟩
    - ☑ Web Bookmarks
    - ☑ Web Cache
    - ☑ Web Cookies Accessed
    - ☑ Web Cookies Create

Date/Time	Event Type	Description	Tagged	Hash Hit
2001-12-12 16:10:54	Document Created	Document Created : :		
2003-02-04 20:11:17	Document Created	Document Created : :		
2003-07-10 13:33:15	Document Created	Document Created : :		
2003-07-10 15:17:56	Document Created	Document Created : :		
2003-07-10 17:37:13	Document Last Saved	Document Last Saved : :		
2003-09-24 15:33:42	Exif	Eastman Kodak Company : KODAK DIGITAL SCIENCE DC260 (V01.00) : image_13.jpg		
2003-11-25 00:09:57	Document Created	Document Created : :		
2003-12-10 17:27:44	Exif	Eastman Kodak Company : KODAK DIGITAL SCIENCE DC260 (V01.00) : image_113.jpg		
2004-02-20 06:53:23	Document Created	Document Created : :		
2004-05-06 01:10:13	Document Created	Document Created : :		
2004-10-05 14:50:21	Document Created	Document Created : :		
2004-10-06 10:46:47	Exif	EASTMAN KODAK COMPANY : KODAK DX4530 ZOOM DIGITAL CAMERA : f0439240.jpg		
2004-10-07 07:24:19	Exif	EASTMAN KODAK COMPANY : KODAK DX4530 ZO EASTMAN KODAK COMPANY : KODAK DX4530 ZOOM DIGITAL CAMERA : f0439240.jpg		
2004-10-07 11:55:46	Exif	EASTMAN KODAK COMPANY : KODAK DX4530 ZOOM DIGITAL CAMERA : f0506536.jpg		
2005-04-04 04:00:33	Exif	EASTMAN KODAK COMPANY : KODAK DX4530 ZOOM DIGITAL CAMERA : f0504872.jpg		
2005-04-04 05:41:46	Exif	EASTMAN KODAK COMPANY : KODAK DX4530 ZOOM DIGITAL CAMERA : f0502376.jpg		
2005-12-03 16:53:25	Document Created	Document Created : :		
2006-01-05 16:52:42	Document Last Saved	Document Last Saved : :		
2006-03-13 17:15:18	Document Last Saved	Document Last Saved : :		
2006-03-21 19:00:00	Document Created	Document Created : :		
2006-03-21 19:02:00	Document Last Saved	Document Last Saved : :		

Start: Dec 12, 2001, 4:10:54 PM   Jump By: year   End: Feb 6, 2015, 8:04:01 PM

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

ANS รูปส่วยใหญ่เปิดได้ แต่mp4เปิดไม่ได้



- Data Sources
  - cfreds_2015_data_leakage_rm#2.dd_1 Host
    - cfreds_2015_data_leakage_rm#2.dd
      - $CarvedFiles (1)
        - 1 (62)
- File Views
  - File Types
  - Deleted Files
    - File System (0)
    - All (62)
  - MB File Size
- Data Artifacts
  - Metadata (25)
- Analysis Results
  - EXIF Metadata (11)
  - Extension Mismatch Detected (2)
  - Keyword Hits (28)
  - User Content Suspected (11)
- OS Accounts
- Tags
- Score
- Reports

Listing

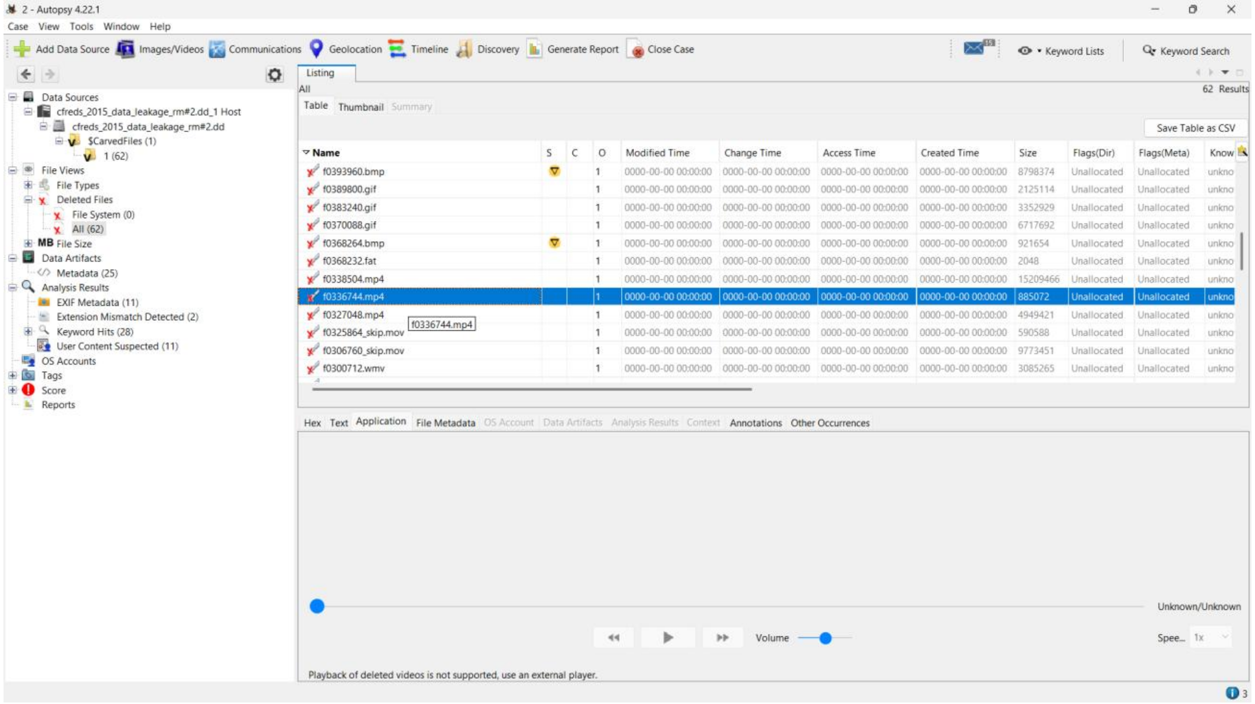
All — 62 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
f0393960.bmp	▽		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	8798374	Unallocated	Unallocated	unkno
f0389800.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	2125114	Unallocated	Unallocated	unkno
f0383240.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	3352929	Unallocated	Unallocated	unkno
f0370088.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	6717692	Unallocated	Unallocated	unkno
f0368264.bmp	▽		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	921654	Unallocated	Unallocated	unkno
f0368232.fat			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	2048	Unallocated	Unallocated	unkno
f0338504.mp4			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	15209466	Unallocated	Unallocated	unkno
f0336744.mp4			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	885072	Unallocated	Unallocated	unkno
f0327048.mp4			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	4949421	Unallocated	Unallocated	unkno
f0325864_skip.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	590588	Unallocated	Unallocated	unkno
f0306760_skip.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	9773451	Unallocated	Unallocated	unkno
f0300712.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	3085265	Unallocated	Unallocated	unkno

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 14% Reset
Tags Menu
03/30/2013
3



- Data Sources
  - cfreds_2015_data_leakage_rm#2.dd_1 Host
    - cfreds_2015_data_leakage_rm#2.dd
      - $CarvedFiles (1)
        - 1 (62)
- File Views
  - File Types
  - Deleted Files
    - File System (0)
    - All (62)
  - MB File Size
- Data Artifacts
  - Metadata (25)
- Analysis Results
  - EXIF Metadata (11)
  - Extension Mismatch Detected (2)
  - Keyword Hits (28)
  - User Content Suspected (11)
- OS Accounts
- Tags
- Score
- Reports

Listing

All — 62 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
f0393960.bmp	▽		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	8798374	Unallocated	Unallocated	unkno
f0389800.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	2125114	Unallocated	Unallocated	unkno
f0383240.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	3352929	Unallocated	Unallocated	unkno
f0370088.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	6717692	Unallocated	Unallocated	unkno
f0368264.bmp	▽		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	921654	Unallocated	Unallocated	unkno
f0368232.fat			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	2048	Unallocated	Unallocated	unkno
f0338504.mp4			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	15209466	Unallocated	Unallocated	unkno
f0336744.mp4			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	885072	Unallocated	Unallocated	unkno
f0327048.mp4			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	4949421	Unallocated	Unallocated	unkno
f0325864_skip.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	590588	Unallocated	Unallocated	unkno
f0306760_skip.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	9773451	Unallocated	Unallocated	unkno
f0300712.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	3085265	Unallocated	Unallocated	unkno

f0336744.mp4
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Unknown/Unknown
Volume
Spee... 1x
3

Playback of deleted videos is not supported, use an external player.

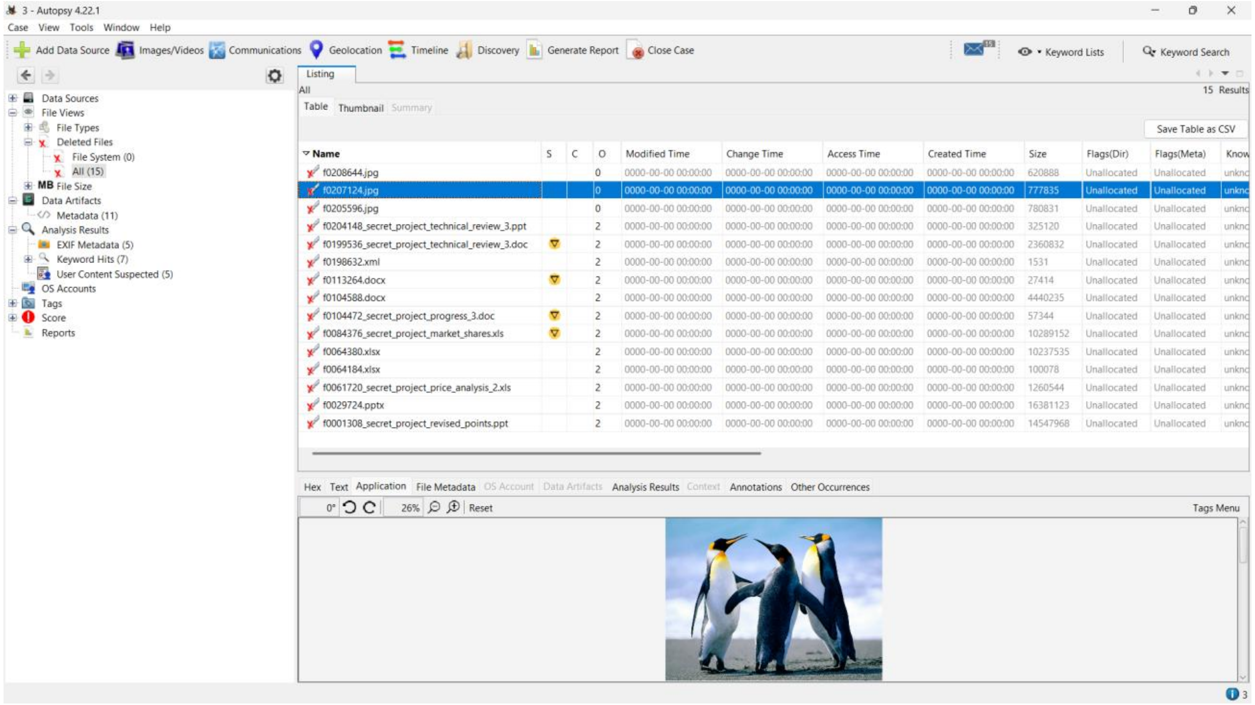
4. What actions were performed for anti-forensics on USB drive ‘RM#2’?

[Hint: this can be inferred from the results of the above question]

ANS ทั้งมีการพยายามลบหลักฐานทิ้ง และ มีการปลอมแปลงฟอร์แมตไฟล์ สังเกตว่า มีชื่อไฟล์แปลกๆที่ตั้งชื่อลงท้ายด้วย .txt แต่เนื้อหาข้างในไม่น่าใช่ จึงลองเปลี่ยน TYPE เป็น .ppt

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

ANS found 15 files



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
f0208644.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	620888	Unallocated	Unallocated	unknc
f0207124.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	777835	Unallocated	Unallocated	unknc
f0205596.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	780831	Unallocated	Unallocated	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc
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	unknc

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

ANS น่าจะแค่ลบไฟล์ทำลายหลักฐานทิ้ง มั้ง