

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 เมื่อผู้ใช้ลบไฟล์ ระบบปฏิบัติการจะดำเนินการเพียงแค่ ลบหรือทำลาย Metadata 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

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_Phudent_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 อย่างน้อย 7 รอบ ประมาณ 14 ชั่วโมง 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 found 55 events

Timeline - Editor

Display Times In: Local Time Zone GMT / UTC

View Mode: Counts Details List

55 events

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 ZOOM DIGITAL CAMERA : f0508296.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 : :		

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

ANS I don't know what do ya mean traversed and opened?

Timeline - Editor

Display Times In: Local Time Zone GMT / UTC

View Mode: Counts Details List

55 events

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 ZOOM DIGITAL CAMERA : f0508296.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 : :		

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

ANS รูปสวยใหญ่เปิดได้ แต่mp4เปิดไม่ได้

Autopsy 4.22.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing 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
R0393960.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
R0389800.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
R0383240.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
R0370088.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
R0368264.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
R0368232.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
R0338504.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
R0336744.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
R0327048.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
R0325864_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
R0306760_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
R0300712.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

Tags Menu

0% 14% Reset



Autopsy 4.22.1

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing 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
R0393960.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
R0389800.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
R0383240.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
R0370088.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
R0368264.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
R0368232.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
R0338504.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
R0336744.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
R0327048.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
R0325864_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
R0306760_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
R0300712.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

Unknown/Unknown

Spee... 1x

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)	Known
0208644.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	Unknown
0207124.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	Unknown
0205596.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	Unknown
0204148_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
0199536_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
0198632.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
0113264.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
0104588.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
0104472_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
0084376_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
0064380.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
0064184.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
0061720_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
0029724.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
0001308_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

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

ANS น่าจะแค่ลบไฟล์ทำลายหลักฐานทิ้ง มั้ง