

# Activity: Computer Forensics

## 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.

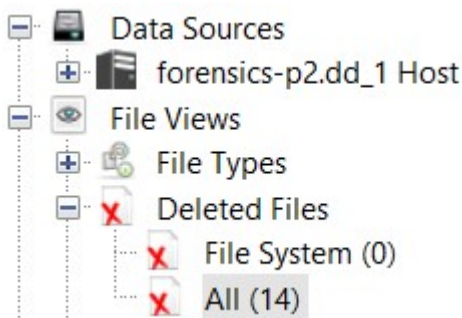
**Ans**

Name	MIME Type	S	C	O	Modified Time	Change Time	Access Time
f0000281_Nick_is_a_pretty_man_with_a_2003_docur	application/msword			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000321.wmv	video/x-ms-wmv			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0016021.wav	audio/vnd.wave			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0016693.xls	application/vnd.ms-excel			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0016741_Prudent_Engineering_Practice_for_Crypto	application/pdf		▼	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0019477.pdf	application/pdf			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0019717.jpg	image/jpeg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0019777.jpg	image/jpeg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0020645.jpg	image/jpeg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0020841.gif	image/gif			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0020853_moov.mov	video/quicktime			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0021929.wmv	video/x-ms-wmv			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0023957.ppt	application/vnd.ms-powerpoint			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0023981_wword60.zip	application/zip			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Based on the picture, all sections are marked as "unallocated," meaning the system can write to those areas. However, the contents of the deleted files are not actually erased. By using a tool or method, such as Autopsy, you can recover and list deleted files that are marked as "unallocated."

2. How many objects can you find?

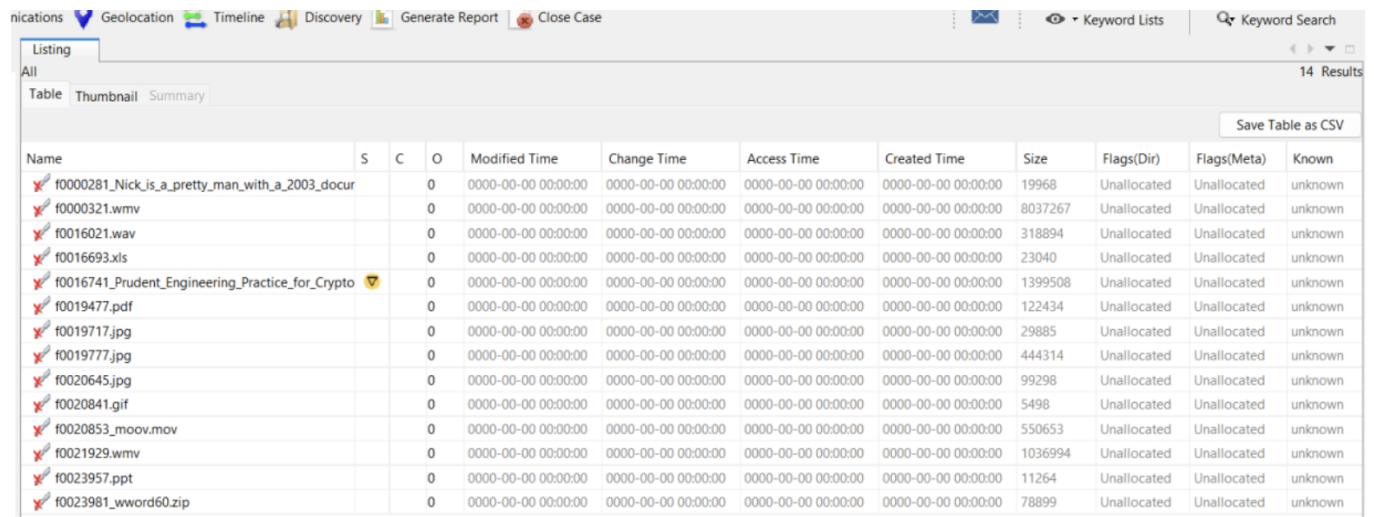
**Ans** 14 files



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.

### Ans

According to the image, all files are marked as "unallocated," and no files are damaged, corrupted, or actually deleted.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
f0000281_Nick_is_a_pretty_man_with_a_2003_docur			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
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
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	318894	Unallocated	Unallocated	unknown
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
f0016741_Prudent_Engineering_Practice_for_Crypto			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
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
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
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
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
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
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
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
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
f0023981_wword60.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

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?

### Ans

To completely delete a file from an HDD, overwrite it at least once with random data. For higher security, use 3 passes (following the DoD standard). More passes (like 7) are generally overkill for modern drives.

To ensure files are fully deleted on a magnetic hard disk, I will use 3 passes for this calculation.

For a single-pass overwrite on a modern HDD with a write speed of 150 MB/s:

1 TB = 1,000,000 MB

Time = 1,000,000 MB / 150 MB/s  $\approx$  6,667 seconds  $\approx$  1.85 hours

Thus, for 3 passes:

Total time = 1.85 hours x 3  $\approx$  5.55 hours

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

### Ans

When a file is deleted on an SSD, it may not be in its original location or may be replaced by new data, making it difficult for file carving techniques to recover it. Additionally, SSDs often use TRIM commands to

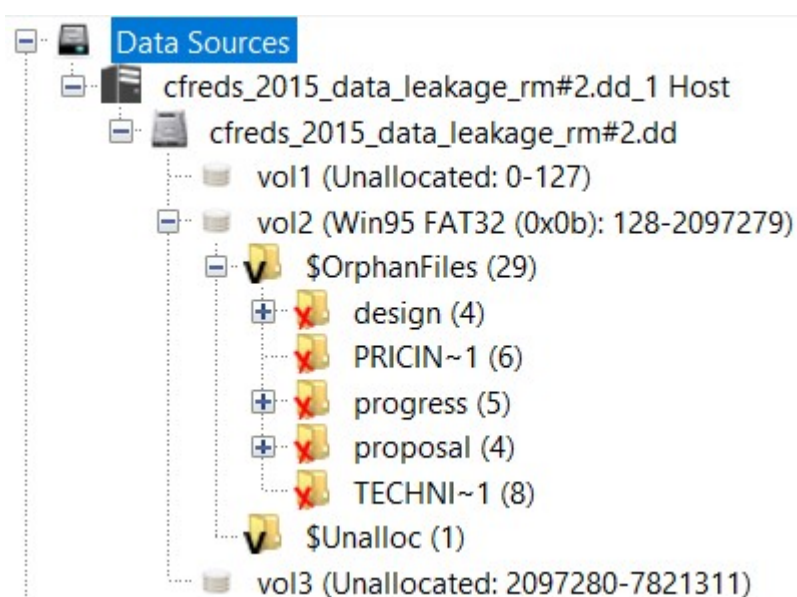
inform the drive that sectors are no longer in use, which can result in immediate and permanent deletion of the file's data.

## Part II. Investigation

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













































### Ans

1. design
2. PRICIN~1
3. progress
4. proposal
5. TeCHNI~1


















## 2. List all files that were opened in 'RM#2'. 5 Computer Security Dept. of Computer Engineering Chulalongkorn University

### Ans

2015-03-23 00:00:00	 A__	/OrphanFiles/injera.gif		
2015-03-23 00:00:00	 A__	/OrphanFiles/amalfi.bmp		
2015-03-23 00:00:00	 A__	/OrphanFiles/JACK-O~1.TIF		
2015-03-23 00:00:00	 A__	/OrphanFiles/oak-snow.jpg		
2015-03-23 00:00:00	 A__	/OrphanFiles/leaf.jpg		
2015-03-23 00:00:00	 A__	/OrphanFiles/blini.gif		
2015-03-23 00:00:00	 A__	/OrphanFiles/BAMBOO~1.GIF		
2015-03-23 00:00:00	 A__	/OrphanFiles/orchid.png		
2015-03-23 00:00:00	 A__	/OrphanFiles/boudicca.bmp		
2015-03-23 00:00:00	 A__	/OrphanFiles/barn.gif		
2015-03-23 00:00:00	 A__	/OrphanFiles/wat.gif		
2015-03-23 00:00:00	 A__	/OrphanFiles/STONEH~1.JPG		
2015-03-23 00:00:00	 A__	/OrphanFiles/PIAZZA~1.JPG		
2015-03-23 00:00:00	 A__	/OrphanFiles/cave.png		
2015-03-23 00:00:00	 A__	/OrphanFiles/SPQR.JPG		
2015-03-23 00:00:00	 A__	/OrphanFiles/cactus.png		
2015-03-23 00:00:00	 A__	/OrphanFiles/eggs.gif		
2015-03-23 00:00:00	 A__	/OrphanFiles/tomatoes.gif		
2015-03-23 00:00:00	 A__	/OrphanFiles/tapas.gif		
2015-03-23 00:00:00	 A__	/OrphanFiles/CUTTY~1.JPG		
2015-03-23 00:00:00	 A__	/OrphanFiles/pisa.JPG		
2015-03-23 00:00:00	 A__	/OrphanFiles/FORSYT~1.PNG		
2015-03-23 00:00:00	 A__	/OrphanFiles/jump.jpg		
2015-03-24 00:00:00	 A__	/OrphanFiles/TECHNI~1/diary_#2d.txt		
2015-03-24 00:00:00	 A__	/OrphanFiles/TECHNI~1/diary_#2p.txt		
2015-03-24 00:00:00	 A__	/OrphanFiles/TECHNI~1/diary_#1d.txt		
2015-03-24 00:00:00	 A__	/OrphanFiles/TECHNI~1/diary_#3p.txt		
2015-03-24 00:00:00	 A__	/OrphanFiles/design		
2015-03-24 00:00:00	 A__	/OrphanFiles/PRICIN~1/super_bowl.avi		
2015-03-24 00:00:00	 A__	/OrphanFiles/desktop.ini		
2015-03-24 00:00:00	 A__	/OrphanFiles/TECHNI~1/diary_#1p.txt		
2015-03-24 00:00:00	 A__	/OrphanFiles/progress		
2015-03-24 00:00:00	 A__	/OrphanFiles/design/winter_whether_advisory.zip		
2015-03-24 00:00:00	 A__	/OrphanFiles/TECHNI~1		
2015-03-24 00:00:00	 A__	/OrphanFiles/PRICIN~1		
2015-03-24 00:00:00	 A__	/OrphanFiles/proposal		
2015-03-24 00:00:00	 A__	/OrphanFiles/TECHNI~1/diary_#3d.txt		
2015-03-24 00:00:00	 A__	/OrphanFiles/progress/new_year_calendar.one		
2015-03-24 00:00:00	 A__	/OrphanFiles/progress/my_smartphone.png		
2015-03-24 00:00:00	 A__	/OrphanFiles/proposal/landscape.png		
2015-03-24 00:00:00	 A__	/OrphanFiles/proposal/a_gift_from_you.gif		
2015-03-24 00:00:00	 A__	/OrphanFiles/PRICIN~1/new_years_day.jpg		
2015-03-24 00:00:00	 A__	/OrphanFiles/progress/my_friends.svg		
2015-03-24 00:00:00	 A__	/OrphanFiles/design/winter_storm.amr		
2015-03-24 00:00:00	 A__	/OrphanFiles/PRICIN~1/my_favorite_cars.db		
2015-03-24 00:00:00	 A__	/OrphanFiles/PRICIN~1/my_favorite_movies.7z		

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

Ans

Name	▼ MIME Type
 a_gift_from_you.gif	application/vnd.openxmlformats-officedocument.word..
 landscape.png	application/vnd.openxmlformats-officedocument.word..
 diary_#1d.txt	application/vnd.openxmlformats-officedocument.word..
 diary_#2d.txt	application/vnd.openxmlformats-officedocument.word..
 my_favorite_movies.7z	application/vnd.openxmlformats-officedocument.sprea..
 new_years_day.jpg	application/vnd.openxmlformats-officedocument.sprea..
 winter_whether_advisory.zip	application/vnd.openxmlformats-officedocument.prese..
 diary_#1p.txt	application/vnd.openxmlformats-officedocument.prese..
 winter_storm.amr	application/vnd.ms-powerpoint
 diary_#2p.txt	application/vnd.ms-powerpoint
 diary_#3p.txt	application/vnd.ms-powerpoint
 my_favorite_cars.db	application/vnd.ms-excel
 super_bowl.avi	application/vnd.ms-excel
 amalfi.bmp	application/octet-stream
 BAMBOO~1.GIF	application/octet-stream

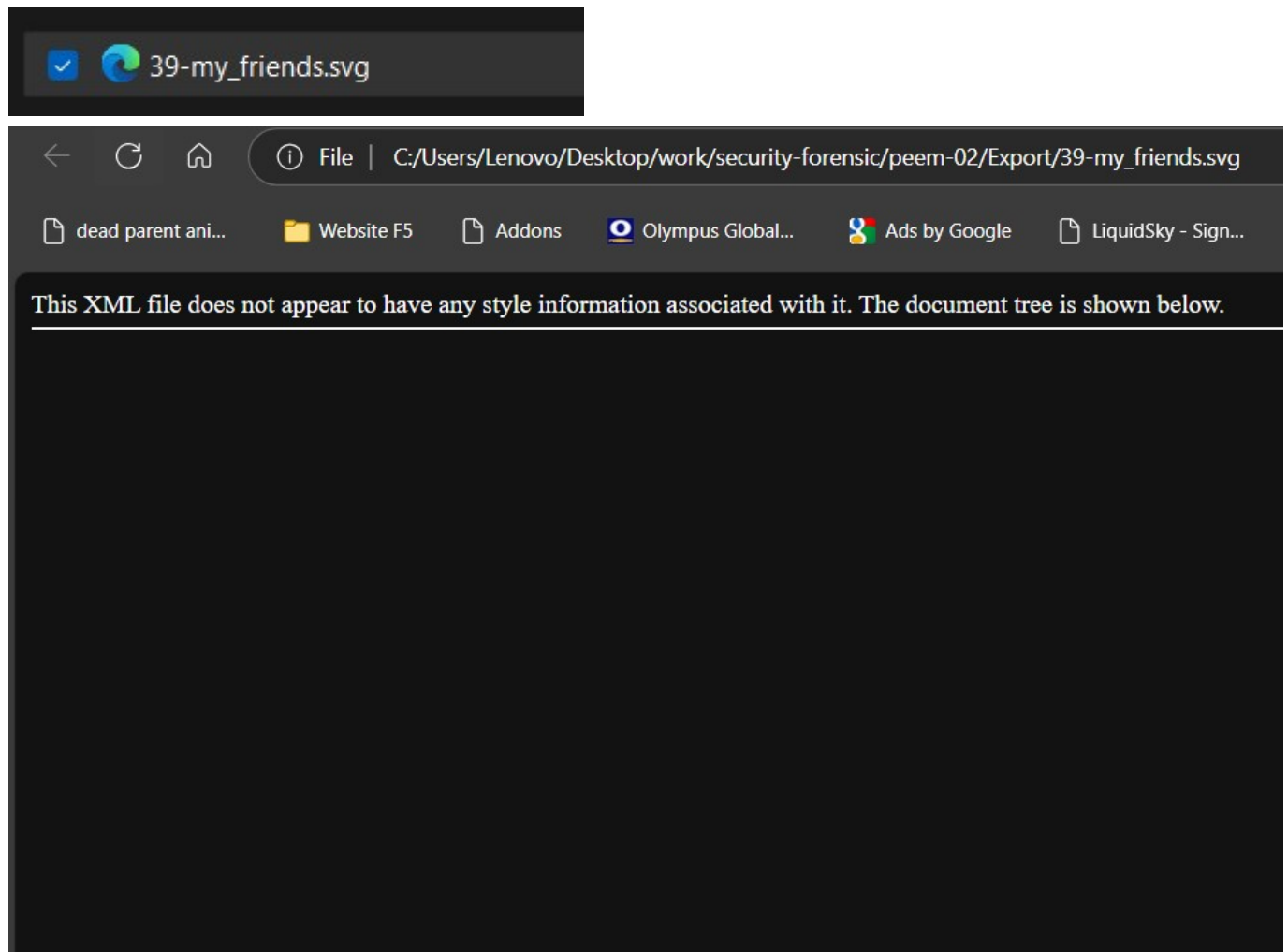


#### 4. What actions were performed for anti-forensics on USB drive 'RM#2'? [Hint: this can be inferred from the results of the above question]

##### Ans

For anti-forensics on USB drive 'RM#2', the action performed was changing the file extension to make it not match the MIME type. This makes it more challenging to identify and recover the file using file carving techniques, as the file's extension no longer reflects its true content type.

- After restoring the file and trying to open it, the file cannot be read.



- From the metadata, we know that this file is of MS Word type.



- Tried changing the file extension to match the MIME type.



39-my\_friends.doc

# [Secret Project]
















## Progress #3.doc

This file is one of Govdocs (<http://digitalcorpora.org/corpora/govdocs>)  
The first page is added by NIST CFReDS project.  
All following pages have no connection with to the scenario.

Examine media #3.

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

Ans

<input type="checkbox"/>		5-f0001308_secret_project_revised_...	9/16/2024 7:13 PM	Microsoft PowerPo...	14,211 KB
<input type="checkbox"/>		6-f0029724.pptx	9/16/2024 7:13 PM	Microsoft PowerPo...	15,998 KB
<input type="checkbox"/>		7-f0061720_secret_project_price_an...	9/16/2024 7:13 PM	Microsoft Excel 97...	1,231 KB
<input type="checkbox"/>		8-f0064184.xlsx	9/16/2024 7:13 PM	Microsoft Excel W...	98 KB
<input type="checkbox"/>		9-f0064380.xlsx	9/16/2024 7:13 PM	Microsoft Excel W...	9,998 KB
<input type="checkbox"/>		10-f0084376_secret_project_market...	9/16/2024 7:13 PM	Microsoft Excel 97...	10,048 KB
<input type="checkbox"/>		11-f0104472_secret_project_progre...	9/16/2024 7:13 PM	Microsoft Word 97...	56 KB
<input type="checkbox"/>		12-f0104588.docx	9/16/2024 7:13 PM	Microsoft Word D...	4,337 KB
<input type="checkbox"/>		13-f0113264.docx	9/16/2024 7:13 PM	Microsoft Word D...	27 KB
<input type="checkbox"/>		14-f0198632.xml	9/16/2024 7:13 PM	XML Source File	2 KB
<input type="checkbox"/>		15-f0199536_secret_project_technic...	9/16/2024 7:13 PM	Microsoft Word 97...	2,306 KB
<input type="checkbox"/>		16-f0204148_secret_project_technic...	9/16/2024 7:13 PM	Microsoft PowerPo...	318 KB
<input type="checkbox"/>		17-f0205596.jpg	9/16/2024 7:13 PM	JPG File	763 KB
<input type="checkbox"/>		18-f0207124.jpg	9/16/2024 7:13 PM	JPG File	760 KB
<input type="checkbox"/>		19-f0208644.jpg	9/16/2024 7:13 PM	JPG File	607 KB



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

Ans

Changed the file name to make it unrelated to the content of the file.



[Secret Project]

price\_analysis\_#1.xlsx