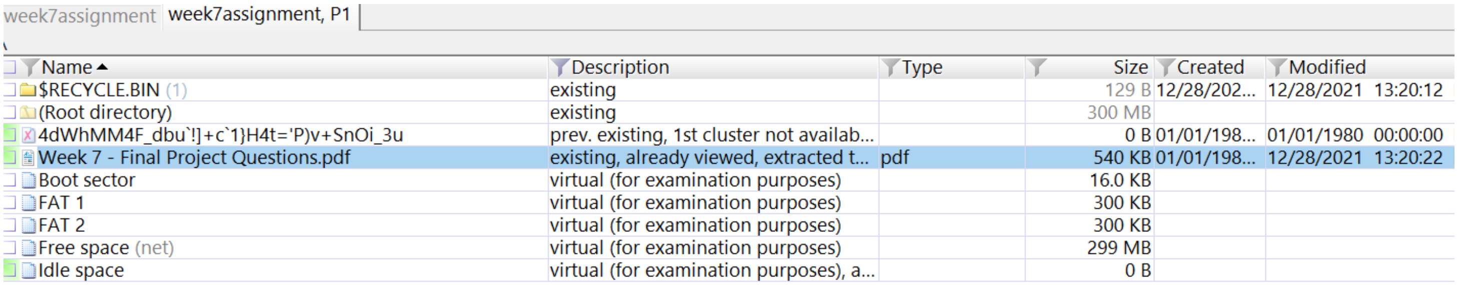
THE SUMMIT

CFDI 320-45A

Ronna Curelea

Question 1:
Search the week7assignment.dd file for any PDF files and extract any findings.



Name	Description	Type	Size	Created	Modified
$RECYCLE.BIN (1)	existing		129 B	12/28/202...	12/28/2021 13:20:12
(Root directory)	existing		300 MB		
4dWhMM4F_dbu`!]+c`1}H4t='P)v+SnOi_3u	prev. existing, 1st cluster not availab...		0 B	01/01/198...	01/01/1980 00:00:00
Week 7 - Final Project Questions.pdf	existing, already viewed, extracted t...	pdf	540 KB	01/01/198...	12/28/2021 13:20:22
Boot sector	virtual (for examination purposes)		16.0 KB		
FAT 1	virtual (for examination purposes)		300 KB		
FAT 2	virtual (for examination purposes)		300 KB		
Free space (net)	virtual (for examination purposes)		299 MB		
Idle space	virtual (for examination purposes), a...		0 B		

Question 2:
Search each partition and locate all PDF files. Create a table that identifies the total number of allocated and unallocated PDF files in each partition.

File	Filetype	Allocation
ApolloDescentGuidance.pdf	NTFS	Allocated
LLRV-DFRC.pdf	NTFS	Allocated
LEM-GNCStudyGuide.pdf	NTFS	Unallocated
e.PDF	Ext4	Allocated
LM-intro.pdf	Ext4	Allocated
LM_Landing Gear1973010151.pdf	Ext4	Allocated
Week 7 - Final Project Questions.pdf	FAT32	Allocated

Question 3:
Carve for JPG/JPEG image files throughout the entire forensic image. How many files were located? 17

Question 4:
Use psteal.exe from the Plaso/Log2Timeline Toolkit and create a basic full timeline across the entire forensic image. Do not specify any unique options.

- *Open the results in Microsoft Excel*
- *Filter and search the data for the file s65-20742_0.jpg. Report on all timestamp information associated with this file.*

Metadata Modification Time:	06/23/2020 20:45:29
Content Modification Time:	11/14/2028 22:30:46
Last Accessed Time:	06/23/2020 20:45:29
Created Time:	06/23/2020 20:45:29

- *Filter and search the data for the file 574254main_archivelaunch.jpg. Report on all timestamp information associated with this file.*

Creation Time:	1/1/1970 0:00:00
Content Modification Time:	6/23/2020 20:46:24

Question 5:
Using The Sleuth Kit, what is the allocated file size reported for the file s65-20742_0.jpg?

466944 bytes = 0.47 megabytes

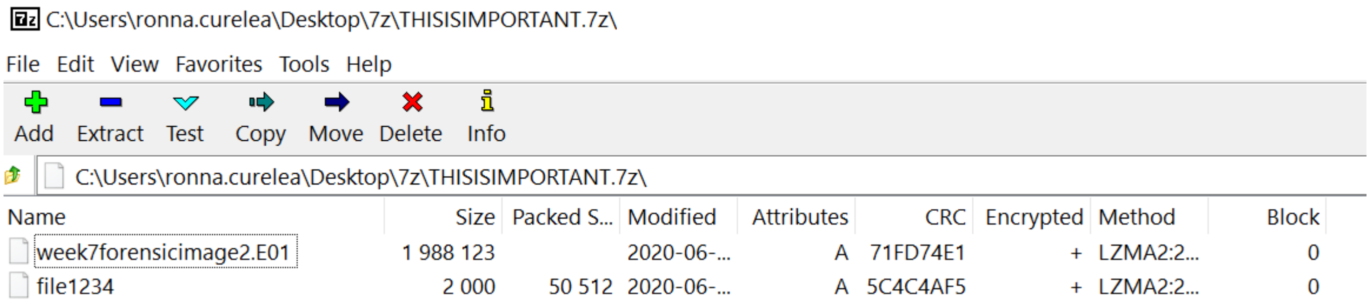
Question 6:
Extract the file s65-20742_0.jpg and review the contents.
Write a few sentences on the contents of this file.

A rocket on a launching pad that is launching into space. There is a lot of combustion and smoke.

Question 7:
Examine each partition for evidence for any evidence of a 7zip file. A 7zip file can be identified by a .7z file extension. If the file is in an NTFS partition, what is the MFT File Record Entry number?
If the file is in an Ext4 partition, what is the inode number?

It’s and Ext4 and the inode is 37.

Question 8: Extract the 7zip file and open it. The password is the total sum of each of the starting offset values for the three partitions. Extract all contents of this archive. Bring a screenshot into this report of the results of you extracting this archive into a folder on your desktop.



C:\Users\ronna.curelea\Desktop\7z\THISISIMPORTANT.7z\

C:\Users\ronna.curelea\Desktop\7z\THISISIMPORTANT.7z\

Name	Size	Packed S...	Modified	Attributes	CRC	Encrypted	Method	Block
week7forensicimage2.E01	1 988 123		2020-06-...	A	71FD74E1	+	LZMA2:2...	0
file1234	2 000	50 512	2020-06-...	A	5C4C4AF5	+	LZMA2:2...	0

Question 9: Open the file titled file1234 in X-Ways Forensics (XWF). Do not interpret this file as a disk. Conduct a sweep at the following locations. The result of this work creates a sentence. What is that sentence?

1 0xE0 1-BYTE
2 0x5C0 4-BYTES
3 0x2F6 4-BYTES
4 0x156 6-BYTES
5 0x69E 9-BYTES

ANSWER: "I LOVE FILE SYSTEM FORENSICS "

Question 10:

Examine the forensic image you extracted from the 7zip archive.
What is the volume name of the 3rd partition?

File System Type: Ext4
Volume Name: THIRD
Volume ID: f9bed6f9ff1d8ea9e84fe9808a2a5309