ITMS 538 Assignment 04b_rds

Alan Palayil

Due Date: 10/16/2022

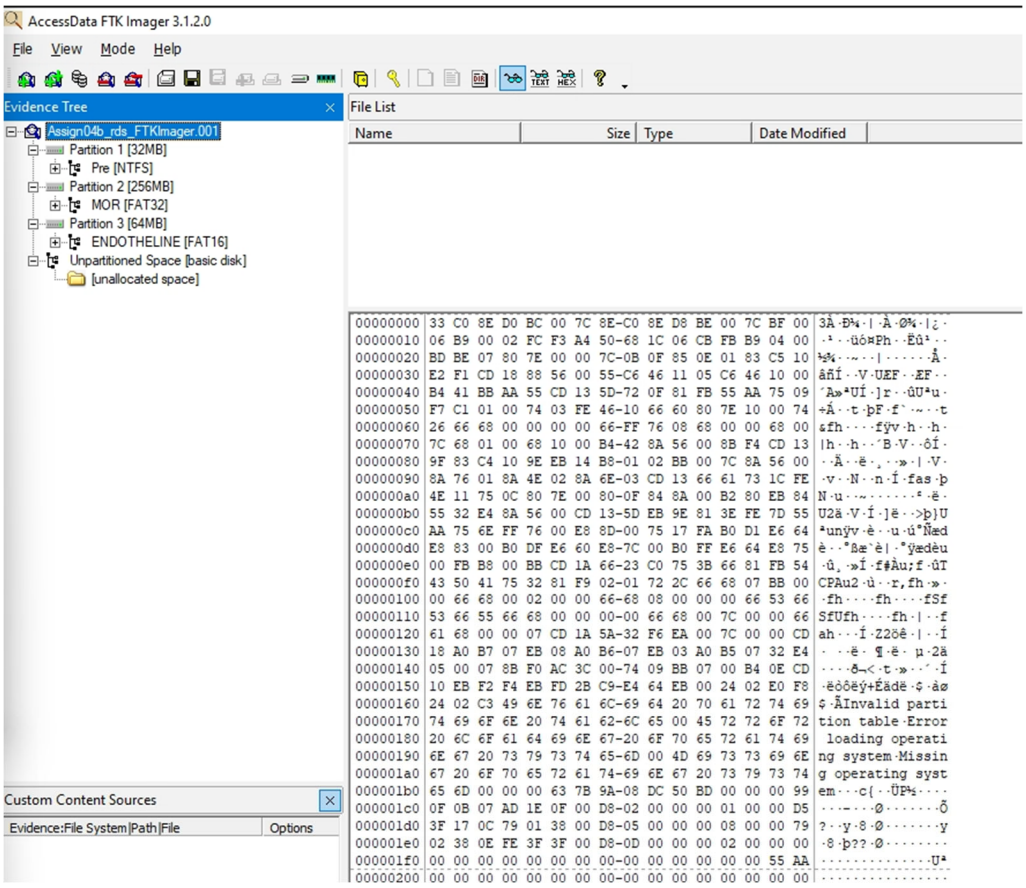
In this assignment, we are tasked to analyze a raw disk image file. We are introduced to various tools and follow the instructions in the assignment. The following steps were used to work over this assignment.

Step 1: We log into RADISHng Windows Desktop and set up the forensic tools WinHex and FTK Imager for analyzing the disk image in Windows. We also set up Kali Linux on the VMware Workstation Pro for using forensic tools on linux. The setup of Kali was followed through Lecture 5 and Lecture 6.

Step 2: We copy the Assign04b_rds.dd disk image from R:\share\Assignments\Assign04 folder to the Labs\Assign04b subdirectory in your E: drive.

Step 3: We are told to use at least 3 forensic tools to analyze the disk image and determine the partition layout. We use WinHex and FTK Imager for Windows platform and mmls and gpart for our Linux platform (Kali). On Step 5 to 8 we use WinHex to analyze the disk image.

Step 4a: Using FTK Imager to analyze the disk image. We open FTK Imager as Administrator. We copy and open the disk image. I first verified the copy disk image to check for invalid partitions or files.



ITMS 538 Assignment 04b_rds

Alan Palayil

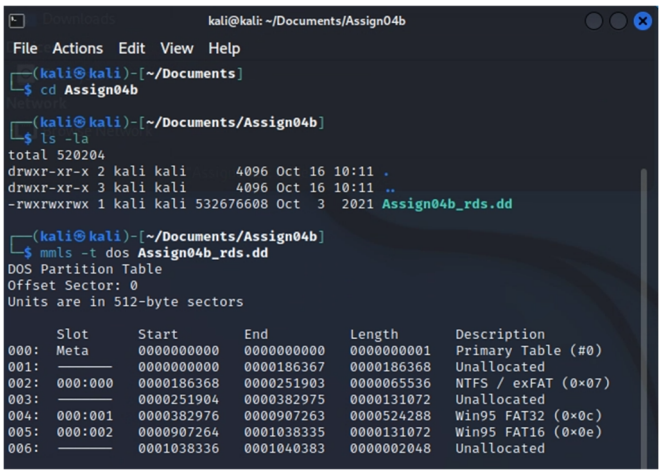
Due Date: 10/16/2022

And expanding the evidence tree we can see 3 partitions of sizes 32MB, 256MB, and 64MB. Expanding each partition shows us the names of the types of partition.

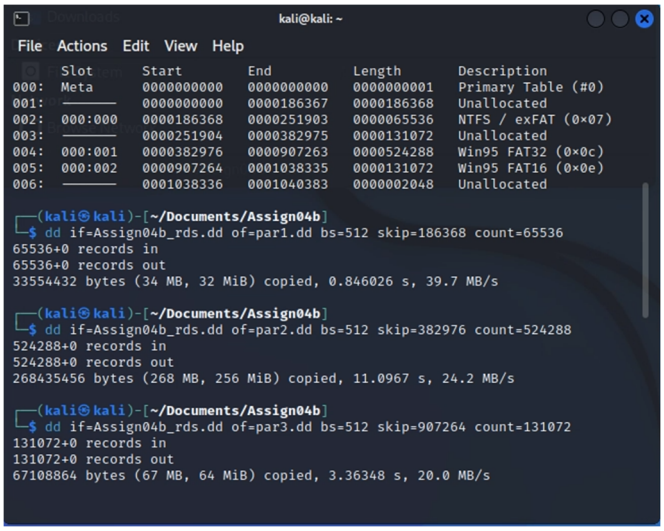
So, for now there are 3 partitions within the disk image excluding the unallocated space.

Step 4b: Using mmls in Kali, we open the terminal. During the Kali setup we have created Share Drives, so we can copy the disk image to a subdirectory in Kali Documents\Assign04b. In the terminal we can navigate to the folder.

We then write the command mmls -t dos Assign04b_rds.dd to display the partitions in the disk image.



We separate each partition using the following commands.

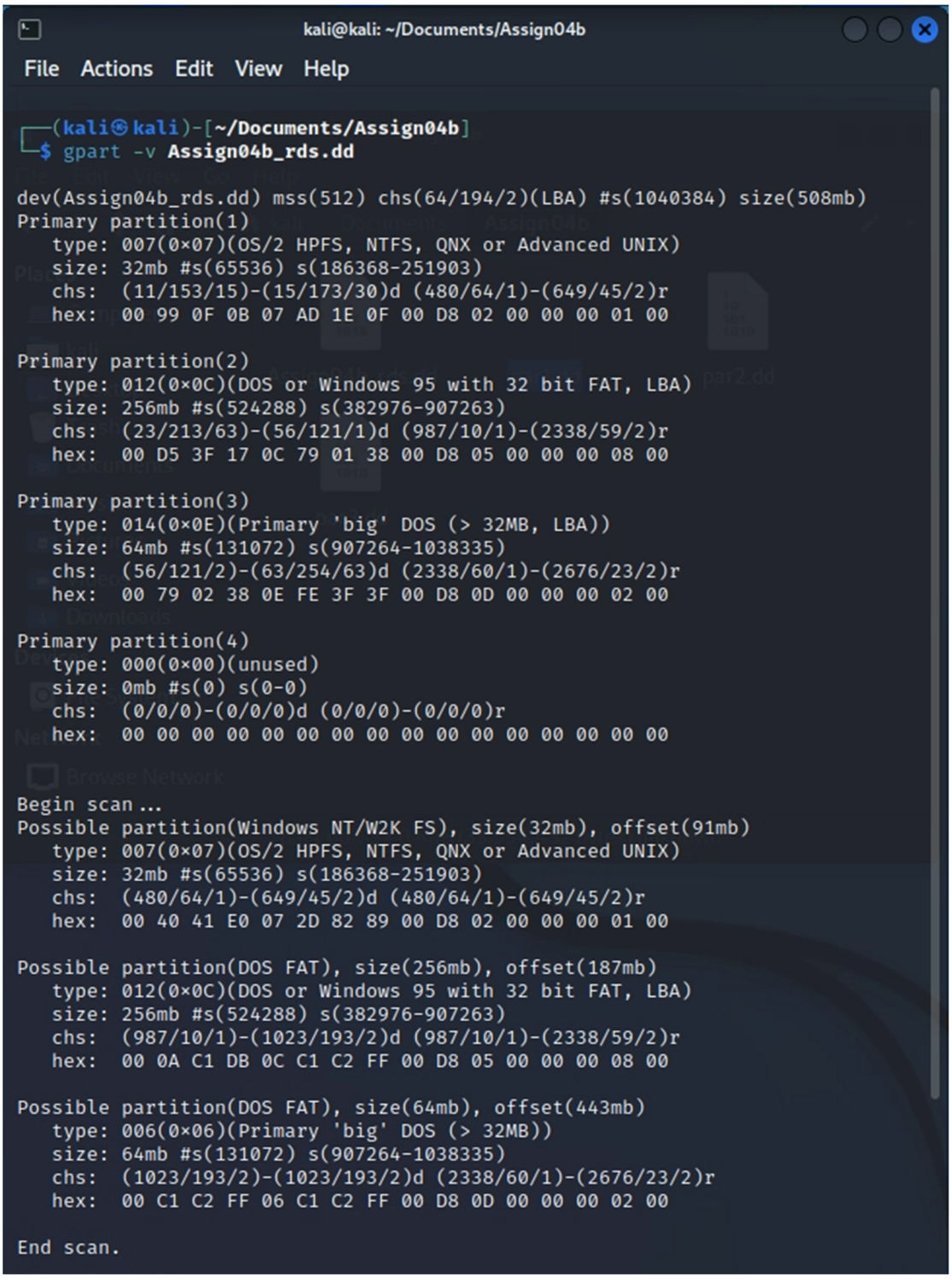


ITMS 538 Assignment 04b_rds

Alan Palayil

Due Date: 10/16/2022

Step 4c: Using gpart in Kali, we can use gpart to get detailed information within each partition to get the LBA Addresses.



ITMS 538 Assignment 04b_rds

Alan Palayil

Due Date: 10/16/2022

```
Guessed primary partition table:
Primary partition(1)
   type: 007(0×07)(OS/2 HPFS, NTFS, QNX or Advanced UNIX)
   size: 32mb #s(65536) s(186368-251903)
   chs:  (480/64/1)-(649/45/2)d (480/64/1)-(649/45/2)r
   hex:  00 40 41 E0 07 2D 82 89 00 D8 02 00 00 00 01 00

Primary partition(2)
   type: 012(0×0C)(DOS or Windows 95 with 32 bit FAT, LBA)
   size: 256mb #s(524288) s(382976-907263)
   chs:  (987/10/1)-(1023/193/2)d (987/10/1)-(2338/59/2)r
   hex:  00 0A C1 DB 0C C1 C2 FF 00 D8 05 00 00 00 08 00

Primary partition(3)
   type: 006(0×06)(Primary 'big' DOS (> 32MB))
   size: 64mb #s(131072) s(907264-1038335)
   chs:  (1023/193/2)-(1023/193/2)d (2338/60/1)-(2676/23/2)r
   hex:  00 C1 C2 FF 06 C1 C2 FF 00 D8 0D 00 00 00 02 00

Primary partition(4)
   type: 000(0×00)(unused)
   size: 0mb #s(0) s(0-0)
   chs:  (0/0/0)-(0/0/0)d (0/0/0)-(0/0/0)r
   hex:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

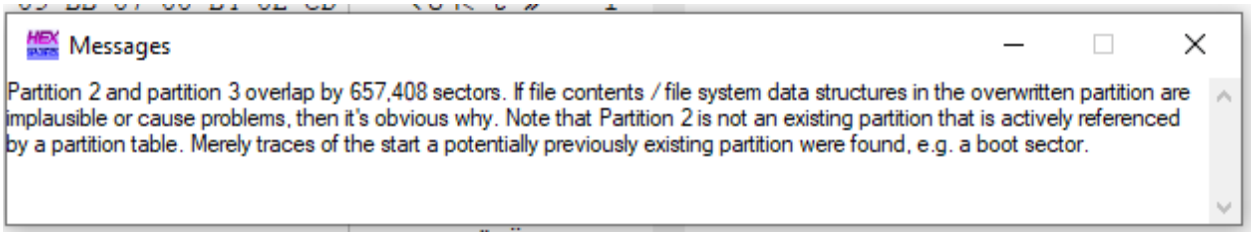
So, using mmls and gpart, we have discovered 4 partitions including Primary boot table, NTFS/ exFAT, Win95 FAT32, and Win95 FAT16 with 2 unallocated spaces.

Step 5: We open WinHex and open the disk image from our Assign04b.

Step 6: When we select the interpret image file as disk and image is read as a disk with all the visible partitions.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Unpartitioned space		91.0 MB					0
Partition 1	NTFS	32.0 MB					186,368
Partition 2	exFAT	385 MB					251,904
Partition 3	FAT32	256 MB					382,976
Partition 4	FAT16	64.0 MB					907,264
Unpartitionable space		64.0 KB					1,040,256

Step 7: While we wait for WinHex to go through the disk image, it creates a partition table, and we encountered the following message.



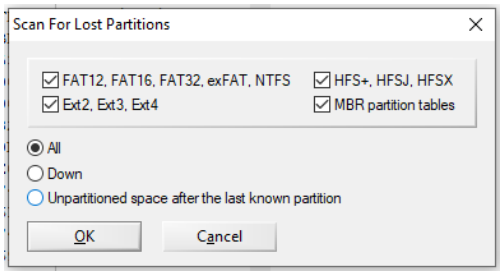
ITMS 538 Assignment 04b_rds

Alan Palayil

Due Date: 10/16/2022

This means that the disk image has invalid partitions and WinHex has not completed the whole scan properly. This leads us to step 8.

Step 8: we go to Disk Tools in Tools menu and rescan the disk for hidden and invalid partitions on WinHex.



After we click OK. We get a refreshed tab with two new partitions 5 and 6 which are in between partition 2 and 4.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Unpartitioned space		91.0 MB					0
Partition 1	NTFS	32.0 MB					186,368
Partition 2	exFAT	385 MB					251,904
Partition 5	exFAT	385 MB					251,916
Partition 3	FAT32	256 MB					382,976
Partition 6	NTFS	64.0 MB					514,048
Partition 4	FAT16	64.0 MB					907,264
Unpartitionable space		64.0 KB					1,040,256

Thus, we have all the 6 partitions within the disk image and below is the determined partition layout like Figure 2. Using template to get the offset measure.

ITMS 538 Assignment 04b_rds

Alan Palayil

Due Date: 10/16/2022

Master Boot Record, Base Offset: 0

Offset	Title	Value
0	Master bootstrap loader	33 C0 8E D0 BC 00 7C 8E C0 8E D8 B
1B8	Windows disk signature	08 DC 50 BD
1B8	Same reversed	BD50DC08

Partition Table Entry #1

1BE	80 = active partition	0
1BF	Start head	153
1C0	Start sector	15
1C0	Start cylinder	11
1C2	Partition type indicator (	07
1C3	End head	173
1C4	End sector	30
1C4	End cylinder	15
1C6	Sectors preceding partiti	186,368
1CA	Sectors in partition 1	65,536

Partition Table Entry #2

1CE	80 = active partition	0
1CF	Start head	213
1D0	Start sector	63
1D0	Start cylinder	23
1D2	Partition type indicator (	0C
1D3	End head	121
1D4	End sector	1
1D4	End cylinder	56
1D6	Sectors preceding partiti	382,976
1DA	Sectors in partition 2	524,288

Partition Table Entry #3

1DE	80 = active partition	0
1DF	Start head	121
1E0	Start sector	2
1E0	Start cylinder	56
1E2	Partition type indicator (	0E
1E3	End head	254
1E4	End sector	63
1E4	End cylinder	63
1E6	Sectors preceding partiti	907,264
1EA	Sectors in partition 3	131,072

Partition Table Entry #4

1EE	80 = active partition	0
1EF	Start head	0
1F0	Start sector	0
1F0	Start cylinder	0
1F2	Partition type indicator (	00
1F3	End head	0
1F4	End sector	0
1F4	End cylinder	0
1F6	Sectors preceding partiti	0
1FA	Sectors in partition 4	0

1FE	Signature (55 AA)	55 AA

ITMS 538 Assignment 04b_rds

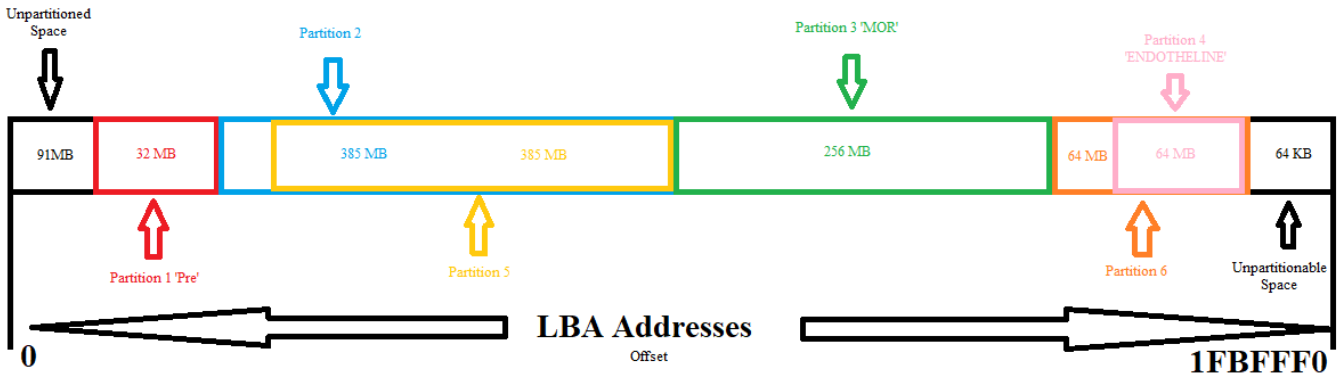
Alan Palayil

Due Date: 10/16/2022

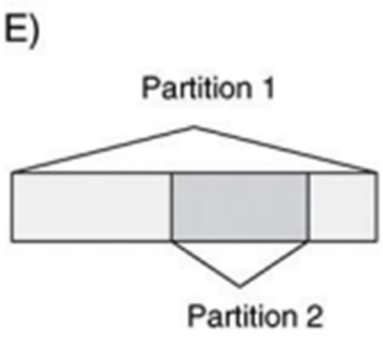
Submittal Answers:

Disk Segments of Assign04b_rds (Using WinHex, FTK Imager, mmls, and gpart)							
LBA Addresses (Offset)		Unallocated?	Name	File System Type	Size	Volume Label	1st Sector
Start	End						
00000000	05AFFFF0	Yes	Unpartitioned Space	N/A	91 MB	N/A	0
05B00000	07AFFFF0	No	Partition 1	NTFS	32 MB	Pre	186368
07B00000	0BAFFFF0	No	Partition 2	exFAT	385 MB	None Found	251904
07B01800	0BAFFFF0	No	Partition 5	exFAT	385 MB	None Found	251916
0BB00000	1BAFFFF0	No	Partition 3	FAT32	256 MB	MOR	382976
0FB00000	1BAFFFF0	No	Partition 6	NTFS	64 MB	None Found	514048
1BB00000	1FBEFFF0	No	Partition 4	FAT16	64 MB	ENDOTHELINE	907264
1FBF0000	1FBFFF0	Yes	Unpartitionable Space	N/A	64 KB	N/A	1040256

Table from Figure 2. And the Disk Image Layout is:



Both the hidden partitions are best exemplified by configuration E for both Partition 5 and 6.



ITMS 538 Assignment 04b_rds

Alan Palayil

Due Date: 10/16/2022

WinHex has a lot more flexibility with disk images in comparison to FTK Imager as you can use forced scan and simulated partition layouts but not get the names of the partitions. While I did not try to use Autopsy, for Windows platform I would prefer to use WinHex. For Kali Linux, gpart tools seems to be briefer in terms of disk partitions, LBA addresses, sectors, and size of each partition. While special command needs to be written for searching hidden/lost partitions. Looking over partition images with gpart -v indicates similar to WinHex if it detects a invalid partition in between.