Volume Analysis[1]

Due Thursday, May 26, 2022 @ 11:59pm
Weight: 15%

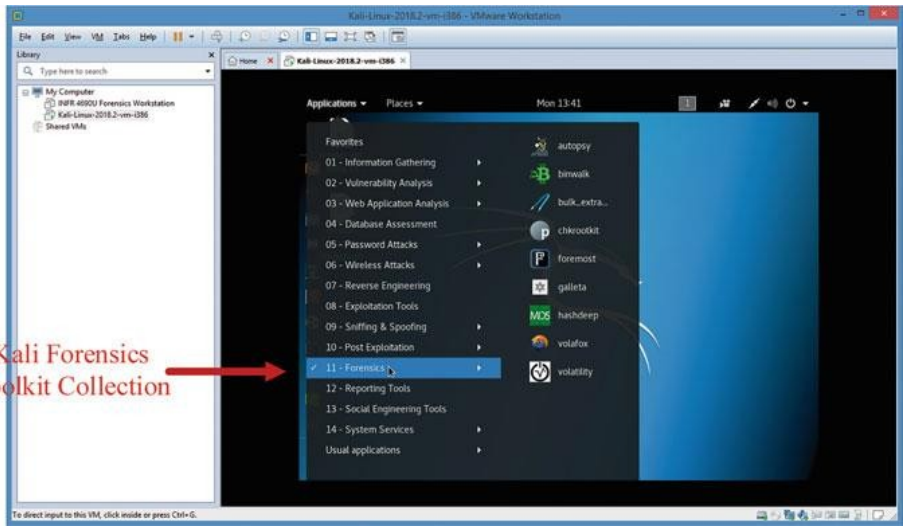
1. Objective

In this lab, you will first learn how to build your own forensics workstation by using some popular open source digital forensics tools, including The Sleuth Kit (TSK) and Autopsy Browser, dcfldd. Then, you will look at the data structures that are involved with partitioning based on two sample disk image files of a popular disk partitioning system, PC-based Partitions (or the master boot record (MBR) partitioning scheme), as used in MS-DOS, Microsoft Windows and Linux on PC compatible computer systems [1,2]. Two sample disk image files include the disk image named "thumbimage_ntfs.dd" provided on the course website in CourseLink and a publicly available extended partition system image [5]. Through examining partition tables, you should be able to know how to conduct a disk volume analysis as well as extract partitions from a disk image. Also, you will start to design and develop you own digital forensic tool, particularly, a volume analysis tool using scripting language like Python, Perl or Linux Shell Scripting.
This lab will be graded, and has to be completed INDIVIDUALLY. After you have finished the tasks, please submit your answers through Courselink

2. Environment Setup

1) Build up your Forensics Workstation with Kali Linux

Please read Chapter 3 of the textbook, build up your Forensics Workstation with Kali Linux onto your computer.



[1] Copyright © 2019 Xiaodong Lin, University of Guelph.
This lab may not be redistributed or used without written permission.

Figure 1. Required Environment Settings

2) Download extended DOS partition testing tool, "**1-extend-part.zip**", where a file called **ext-part-test-2.dd** inside the zip archive (1-extend-part.zip) is a disk image for the purpose of learning extended partition concepts [5], and upload it to your computer forensics workstation.

To download this tool, go to the following link

http://dftt.sourceforge.net/test1/index.html

3) Download the disk image named "**thumbimage_ntfs.dd**" from the course website in the section "**\Datasets\Disk Images**", and upload it to your computer forensics workstation.

3. Exercises (4 marks, 1 mark each)

1) Which of the following statements is not true regarding PC-based Partitions (DOS-style partitions)? (Select One or More Answer Choices) c

a) DOS-style partition systems use MBR (Master Boot Record) to store the partitioning information on a hard disk drive.
b) MBR only holds descriptors for 4 partitions, called the primary partitions. The maximum number of primary partitions supported by MBR is 4.
c) You create a DOS partition (or logical drive), you must be sure to use up all of the hard disk space.
d) MBR contains the disk's partition table and the code to bootstrap an operating system.
e) MBR is located in the first sector of the hard drive.

2) When is the MBR created? c (Select the best answer)
a) Low-level Format
b) High-level Format
c) Partitioning
d) OS Install

3) A partition structure defines how information is structured on the partition, where partitions begin and end, and also the code that is used during startup if a partition is bootable. MBR and GPT are two different ways of storing the partitioning information on a drive. What does GPT stands for? GUID Partition Table,The location information of the partitioned table is stored in the GPT header

4) How big, in bytes, is MBR for 1TB Hard Drive? 512 byte.

4. Hands-on Activities

1) Extract the MBR from the disk image "*thumbimage_ntfs.dd*" (1 mark)

Activities: Extract the MBR from the disk image provided by using the 'dcfldd' tool.

Hint: You have to know the location (the starting point and length) of a MBR in order to extract it.

Writing down your command(s) issued to extract the MBR from "thumbimage_ntfs.dd"?

dcfldd if=thumbimage_ntfs.dd bs=512 skip=0 count=1 of=mbrfat.dd

2) Analyze the disk image "*thumbimage_ntfs.dd*" (1 mark)

Activities: Analyze the disk image provided and fill the following table with the appropriate values in the right column. Except partition entry value and partition type, all other values are in decimal format.

If any partition table entry's 16-byte value is all 0, it means that the corresponding partition doesn't exist. Thus, you don't have to fill in the table for it.

Partition table	
Partition #0 entry value in 16-byte Hexadecimal Format	0003 0200 0707 e0c9 6100 0000 9fc9 0300
Starting CHS address	Cylinder:0, head:3,sector:2
Ending CHS address	Cylinder:201, head:7,sector:224
Starting LBA address	0x00000061 => 97
Number of sectors in partition	248223
size of the partition (MB)	0x0030c99f ×512B = 248233×512B = 121.2026MB
Type of partition	0x07=>NTFS
Partition #1 entry value in 16-byte Hexadecimal Format	
Starting CHS address	
Ending CHS address	
Starting LBA address	
Number of sectors in partition	
size of the partition (MB)	

Type of partition	
Partition #2 entry value in 16-byte Hexadecimal Format	
Starting CHS address	
Ending CHS address	
Starting LBA address	
Number of sectors in partition	
size of the partition (MB)	
Type of partition	
Partition #3 entry value in 16-byte Hexadecimal Format	
Starting CHS address	
Ending CHS address	
Starting LBA address	
Number of sectors in partition	
size of the partition (MB)	
Type of partition	

3) **Extract the partition(s) from the disk image "*thumbimage_ntfs.dd*"** (1 mark)

Activities: Extract the first partition from the disk image provided by using the 'dcfldd' tool.

Hint: You have to know the starting point and length of a partition in order to extract it.

Writing down your command(s) issued to extract the first partition from the disk image "thumbimage_ntfs.dd"?

dcfldd if=thumbimage_ntfs.dd bs=512 skip=97 count=248223 of=firstpartfat.dd

4) **Perform a partition consistency check on disk image (2 marks)**

Activities: Perform a partition consistency check on the disk image "thumbimage_ntfs.dd" and answer the following questions.

Is it possible to hide data on the disk which images are made of?

If yes, please explain why.

Yes, because there may be some storage areas that are not partitioned. If the area is not partitioned, the MBR will not record information about the partition. So there could be hidden information

5) Analyze the Extended DOS Partition Testing Image "*ext-part-test-2.dd*" (8 marks)

Activities: Analyze the Extended DOS Partition testing image "ext-part-test-2.dd" and fill the following tables with the appropriate values in the right column. Except partition record value and partition type, all other values are in decimal format

Primary Partition table	
Partition #0 entry value in 16-byte Hexadecimal Format	0001 0100 041f 3f19 3f00 0000 81cc 0000
Starting CHS address	Cylinder:0, head:1,sector:1
Ending CHS address	Cylinder:25, head:31,sector:63
Starting LBA address	0x0000003f =>63
Number of sectors in partition	52353
size of the partition (MB)	0x0000cc81 * 512B = 52353 * 512B = 25.5630 MB
Type of partition	0x04=>FAT16
Partition #1 entry value in 16-byte Hexadecimal Format	0000 011a 041f 3f33 c0cc 0000 c0cc 0000
Starting CHS address	Cylinder:26, head:0,sector:1

Ending CHS address	Cylinder:51, head:31,sector:63
Starting LBA address	0x0000ccc0=>52416
Number of sectors in partition	52416
size of the partition (MB)	0x0000ccc0 * 512B = 52416 *512B = 25.59375 MB
Type of partition	0x04=>FAT16
Partition #2 entry value in 16-byte Hexadecimal Format	0000 0134 041f 3f4d 8099 0100 c0cc 0000
Starting CHS address	Cylinder:52, head:0,sector:1
Ending CHS address	Cylinder:77, head:31,sector:63
Starting LBA address	0x00019980=>104832
Number of sectors in partition	52416
size of the partition (MB)	0x0000ccc0 * 512B = 52416 *512B = 25.59375 MB
Type of partition	0x04=>FAT16
Partition #3 entry value in 16-byte Hexadecimal Format	0000 014e 051f 3f9a 4066 0200 605e 0200
Starting CHS address	Cylinder:78, head:0,sector:1
Ending CHS address	Cylinder:154, head:31,sector:63
Starting LBA address	0x00026640=>157248
Number of sectors in partition	155232
size of the partition (MB)	0x00025e60 * 512B = 155232 * 512B = 75.796875MB
Type of partition	0x05=>extended

Extended Partition table #1	
Partition #0 entry value in 16-byte Hexadecimal Format	0001 014e 041f 3f67 3f00 0000 81cc 0000
Starting CHS address	Cylinder:78, head:1,sector:1
Ending CHS address	Cylinder:103, head:31,sector:63
Starting LBA address	0x0000003f=>63, 63+157248=157311
Number of sectors in partition	52353
size of the partition (MB)	0x0000cc81*512B = 52353*512B=25.5630MB
Type of partition	0x04=>FAT16
Partition #1 entry value in 16-byte Hexadecimal Format	0001 0168 041f 3f81 ffcc 0000 81cc 0000
Starting CHS address	Cylinder:104, head:1,sector:1

Ending CHS address	Cylinder:129, head:31,sector:63
Starting LBA address	0x0000ccff => 52479,52479+157248=209727
Number of sectors in partition	52353
size of the partition (MB)	0x0000cc81*512B = 52353*512B=25.5630MB
Type of partition	0x04=>FAT16
Partition #2 entry value in 16-byte Hexadecimal Format	0000 0182 051f 3f9a 8099 0100 e0c4 0000
Starting CHS address	Cylinder:130, head:0,sector:1
Ending CHS address	Cylinder:154, head:31,sector:63
Starting LBA address	0x00019980=> 104832,104832+157248=262080
Number of sectors in partition	50400
size of the partition (MB)	0x0000c4e0 *512B = 50400*512B = 24.609375 MB
Type of partition	0x05=>extended
Partition #3 entry value in 16-byte Hexadecimal Format	
Starting CHS address	
Ending CHS address	
Starting LBA address	
Number of sectors in partition	
size of the partition (MB)	
Type of partition	

Extended Partition table #2	
Partition #0 entry value in 16-byte Hexadecimal Format	0001 0182 061f 3f9a 3f00 0000 a1c4 0000
Starting CHS address	Cylinder:130, head:1,sector:1
Ending CHS address	Cylinder:154, head:31,sector:63
Starting LBA address	0x0000003f=>63,63+262080=262143
Number of sectors in partition	50337
size of the partition (MB)	0x0000c4a1*512B=50337*512B=24.57861 MB
Type of partition	0x06=>FAT16
Partition #1 entry value in 16-byte Hexadecimal Format	
Starting CHS address	

Ending CHS address	
Starting LBA address	
Number of sectors in partition	
size of the partition (MB)	
Type of partition	
Partition #2 entry value in 16-byte Hexadecimal Format	
Starting CHS address	
Ending CHS address	
Starting LBA address	
Number of sectors in partition	
size of the partition (MB)	
Type of partition	
Partition #3 entry value in 16-byte Hexadecimal Format	
Starting CHS address	
Ending CHS address	
Starting LBA address	
Number of sectors in partition	
size of the partition (MB)	
Type of partition	

5. Tool Development Activities (3 marks)

In this activity, you are required to complete the following task(s)

1. design and develop a volume analysis tool using scripting language like Python, Perl or Linux Shell Scripting. The tool should
    - list the details of each partition, including Starting CHS address, Starting LBA address, size of the partition (MB), and type of partition;
    - provide partition consistency check, particularly displaying a list of unpartitioned disk space if applicable, which are the space on a hard drive that hasn't been partitioned yet or don't belong to any partition.
2. Output: your program will print out the layout of a disk volume with the following format

    Partitions

    Seq. # Starting CHS Starting LBA Size (MB) Type

Consistency check (Unpartitioned disk space)

Seq. # Starting LBA Size (MB)

where output fields are separated by a **tab** character. Please note that the sequence number (Seq. #) starts with 1. The size in MB is displayed with **three decimal places of precision**.

The following is an example of the output

Partitions

Seq. # Starting CHS Starting LBA Size (MB) Type

1 C:0,H:1,S:1 63 63735.790 NTFS

2 C:1023,H:0,S:0 130530960 88889 NTFS

Consistency check (Unpartitioned disk space)

Seq. # Starting LBA Size (MB)

1 1 0.030

How to Run Your Tool

Assume that your tool is a shell script, called volumeanalysis.sh. Your program should run as follows:

./volumeanalysis.sh disk1.dd

where disk1.dd is a disk image file.

6. What to hand in

By the due date, you are required to hand in:

- A PDF file containing your answers for the questions
- Your volume analysis tool

Create a zip archive with all your deliverables and submit it on CourseLink. The filename must be ass1_XXX.zip, where XXX is your Xidian University Student ID Number (Central Login ID).

You must upload your assignments by email to likicll@163.com.

Appendix A: Structure of a Master Boot Record (MBR)[3]

Address			Description		Size in bytes
Hex	Oct	Dec			
0000	0000	0	Code Area		440 (max. 446)
01B8	0670	440	Optional Disk signature		4
01BC	0674	444	Usually Nulls; 0x0000		2
01BE	0676	446	**Table of primary partitions** (Four 16-byte entries, IBM Partition Table scheme)		64
01FE	0776	510	55h	MBR signature; 0xAA55	2
01FF	0777	511	AAh		
MBR, total size: 446 + 64 + 2 =					512

Appendix B: Layout of one 16-byte partition record[3]

Offset	Field length (bytes)	Description
0x00	1	status (0x80 = bootable (*active*), 0x00 = non-bootable, other = invalid)
0x01	3	CHS address of first block in partition. The format is described in the next 3 bytes.
0x01	1	head
0x02	1	sector is in bits 5–0; bits 9–8 of cylinder are in bits 7–6
0x03	1	bits 7–0 of cylinder
0x04	1	partition type
0x05	3	CHS address of last block in partition. The format is described in the next 3 bytes.
0x05	1	head
0x06	1	sector is in bits 5–0; bits 9–8 of cylinder are in bits 7–6
0x07	1	bits 7–0 of cylinder
0x08	4	LBA of first sector in the partition
0x0C	4	number of blocks in partition, in little-endian format

Appendix C: Some of the type values for DOS partitions[4]

Type	Description
0x00	Empty
0x01	FAT12, CHS
0x04	FAT16, 16–32 MB, CHS
0x05	Microsoft Extended, CHS
0x06	FAT16, 32 MB–2GB, CHS
0x07	NTFS
0x0b	FAT32, CHS
0x0c	FAT32, LBA
0x0e	FAT16, 32 MB–2GB, LBA
0x0f	Microsoft Extended, LBA
0x11	Hidden FAT12, CHS
0x14	Hidden FAT16, 16–32 MB, CHS
0x16	Hidden FAT16, 32 MB–2GB, CHS
0x1b	Hidden FAT32, CHS
0x1c	Hidden FAT32, LBA
0x1e	Hidden FAT16, 32 MB–2GB, LBA
0x42	Microsoft MBR. Dynamic Disk
0x82	Solaris x86
0x82	Linux Swap

Type	Description
0x83	Linux
0x84	Hibernation
0x85	Linux Extended
0x86	NTFS Volume Set
0x87	NTFS Volume Set
0xa0	Hibernation
0xa1	Hibernation
0xa5	FreeBSD
0xa6	OpenBSD
0xa8	Mac OSX
0xa9	NetBSD
0xab	Mac OSX Boot
0xb7	BSDI
0xb8	BSDI swap
0xee	EFI GPT Disk
0xef	EFI System Partition
0xfb	Vmware File System
0xfc	Vmware swap

Reference:

[1] Disk image. http://en.wikipedia.org/wiki/Disk_image
[2] Disk partitioning. [Online] Available at: http://en.wikipedia.org/wiki/Disk_partitioning
[3] Master boot record. [Online] Available at: http://en.wikipedia.org/wiki/Master_boot_record
[4] Brian Carrier. File System Forensic Analysis. Addison-Wesley Professional; 1 edition (Mar 27 2005) ISBN-10: 0321268172
[5] Digital Forensics Tool Testing Images. [Online] Available at: http://dftt.sourceforge.net/
[6] Partitions and Volumes. [Online] Available at: http://www.yale.edu/pclt/BOOT/PARTITIO.HTM