



Analyzing Master Boot Record for Forensic Investigations

Ghania Al Sadi
Sohar University
General Foundation Program
- Computing Program
Sohar, University Rd,
311 - Sultanate of Oman

ABSTRACT

As a main knowledge, extracting information for examination to be used as evidence or even to recover lost data need a full understand of logical and physical storage media structure used to store the required information in the computer. In digital forensic analysis, Master Boot Record is captured to extract the required information of the hard disk to support the investigation process. This research is studying the MBR structure by providing an experiment of the MBR analysis.

General Terms

Master Boot Record, Booting, Forensic Investigation

Keywords

MBR, Bootstrap, Partition Table, Magic Number, Forensic Investigation

1. INTRODUCTION

Master Boot Record (MBR) is the most important part that exists on the first sector (0x00) in the hard drive. It holds the most required terms to boot the device and load the operating system to memory. It is a disk data structure that is created once the disk is partitioned. Disk partition is referred to logical distribution of the hard drive to multiple storage units enabling different file systems to be used on each partition. MBR exists only in partitioned storage devices and cannot be found in non-partitioned disk like floppy disk. MBR consists of the partition table of the disk and finds the bootable disk that is referred as active partitions. Moreover, it holds information related to the type and size of the partitions and the file systems used on each logical partition. In general, MBR is responsible of booting the computer using an

executable code called “bootloader”[1]. MBR supports disks with sectors of 512 bytes that is the currently standard used size. Most disks supported by this partition scheme are limited with two terabyte size[2].

Since MBR is controlling booting process after the BIOS finish its job, make susceptible by malware and some potential threats. Some malicious programs may get control over booting process by altering the MBR and load malicious software to the memory. Moreover, malware like ransomware may move the MBR to different location on the disk and replace itself on the first sector of the disk. Therefore, it carries out the booting process by executing its code once the BIOS switch to the drive for booting. Generally, analyzing MBR is mandatory to extract any malicious programs that may affect the MBR since it carry out the booting process in the computer [3].

For forensic use, investigating the MBR is required since it contains all information about the recent partitions available in the system. Generally, MBR is analyzed to extract storage disks’ information. If the MBR is corrupted, it will be difficult to boot the system and thus difficult to recover data from the storage disks [1].

2. MBR STRUCTURE

MBR is physically located in sector 0(0x00); the first sector in the storage disk that is 512 bytes long. MBR structure consists of three main parts that are master boot code (bootstrap), partition table and the disk signature as shown in Figure 1. All contents of MBR are located in different locations with different number of bytes that need to be fully analyzed to extract the required information [4].

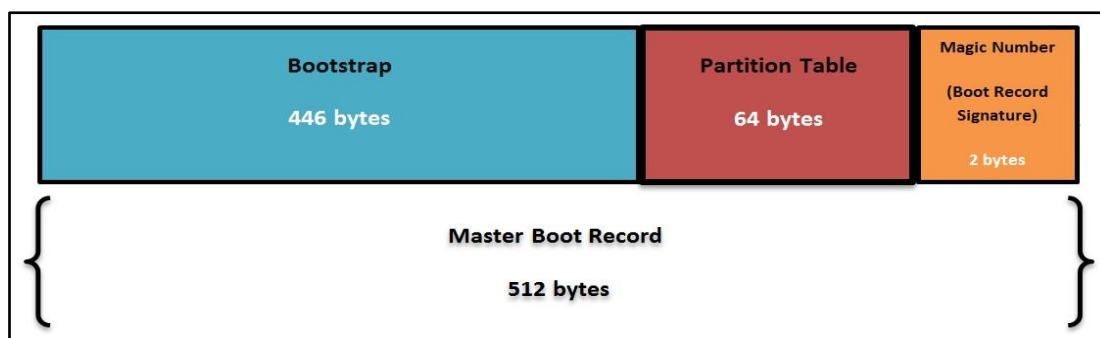


Figure 1: Master Boot Record Structure



2.1 Partition Table

Partition table is a 64 bytes data structure that contains all information of the hard disk partitions. Generally, partitioning the disk to multiple partitions enables different file systems to be used on each partition. Type and location of each partition on the disk is identified by the partition table. The standard number of partitions in the table is four partitions; however the last one might be used as extended partition for other more partition. One of these partitions is marked as an active partition which is used to continue booting process in the computer. The size of the partition table is distributed equally among the four partitions. Normally, each partition table entry begins at predefined offset starting from the beginning of the sector [1].

Partition table is analyzed to find the active partition; that is used to continue booting process. Usually, MBR allows only for one active partition for booting process; however in some cases more than one active partition may exist that cause the MBR to return an error message. Active partition loads files to memory based on the type of the file system used by the partition. In case of missing the active partition, it will be difficult to recover and restore data stored in the disk [5]. Once the active partition is founded, much information may be extracted during analysis process such as the filesystem used by the partition and the size of the partition [1].

2.2 Bootstrap

Bootstrap is referred to as boot loader or Master Boot Code. It is an executable code that is responsible for loading the operating system to computer memory. Bootstrap code area is responsible to find the active partition by scanning the

partition table and catch the first sector in this active partition. Once the active partition is scanned, a copy of the boot sector will be loaded to the memory to start controlling booting process [6]. In case that the master boot code fails to finish its functions, different types of errors will be reported by the system stating some problems with partition table or the operating system either it is not available or error in loading process. Based on the predefined MBR data structure, bootstrap has 446 byte of data structure [2].

2.3 Boot Record Signature

Boot Record Signature is located at the end of the MBR that can be also named as Magic Number. It is a smallest unit in MBR structure that contains only two bytes that is required by the BIOS during booting. The magic number used to report the availability of the boot loader in the hard disk. If the boot loader is located, the magic number value should be (55AA) in hexadecimal calculation [5].

3. MBR ANALYSIS EXPERIMENT

Generally MBR is analyzed to extract or recover required information from the hard disk. Forensic investigations analyze the MBR to find if any malicious MBR exist in the memory that may overwrite the basic or clean MBR. In case of MBR infections, more than one MBR copy may be located in the memory that may be clean or malicious MBR [7]. Therefore, it is mandatory to study the standard MBR structure to distinguish between clean and malicious MBRs. As mentioned before MBR structure consists of 512 bytes distributed among three parts. The following table specifies the specific location of each part in terms of decimal, hex and binary to simplify examining process of the MBR.

Table 1. Master Boot Record Sector Structure

MBR Structure contents		Offsets within MBR Sector		Bytes (length)
		Decimal	Hex	
Bootstrap Code Area		000 – 445	000 – 1BD	446
Partition Table	Partition 1	446 – 461	1BE – 1CD	16
	Partition 2	462 – 477	1CE – 1DD	16
	Partition 3	478 – 493	1DE – 1ED	16
	Partition 4	494 – 509	1EE – 1FD	16
Total of Partition Table		446 – 509	1BE – 1FD	64
Boot Record Signature		510 – 511	1FE – 1FF	2

As described in the table, each pattern exists in a specific offsets within the MBR that are considered as common between different machines. Therefore; finding MBR patterns in different offsets during investigation process will result in potential MBRs in the memory.

A number of tools are used to extract the required information and analyze the MBR that simplify the investigation. Generally, it is important to use an accurate tool to extract evidences from MBR during forensic analysis. In this research, Hex Workshop software is used to analyze the MBR and get accurate information. Hex Workshop it is a powerful hexadecimal tool that is more suitable for investigating sectors

and partition table since it supports decimal, binary and hexadecimal data.

The research is analyzing a previously captured MBR to find Bootstrap Code Area, Active Partition and Boot Record Signature as following:

- **Bootstrap Code Area**

As shown in Figure 2, bootstrap code area is located in the offset (000 – 445) which referred to (000 – 1BD) in hex. Since the bootstrap existing in the correct offset; then it is ready to scan the partition table to find the active partition and load the boot sector into memory.



00000000	33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00 06 B9 00 02 FC
00000015	F3 A4 50 68 1C 06 CB FB B9 04 00 BD BE 07 80 7E 00 00 7C 0B 0F
0000002A	85 0E 01 83 C5 10 E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10
0000003F	00 B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09 F7 C1 01 00
00000054	74 03 FE 46 10 66 60 80 7E 10 00 74 26 66 68 00 00 00 00 66 FF
00000069	76 08 68 00 00 68 00 7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4
0000007E	CD 13 9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00 8A 76 01
00000093	8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE 4E 11 75 0C 80 7E 00 80
000000A8	0F 84 8A 00 B2 80 EB 84 55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E
000000BD	FE 7D 55 AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64 E8 83
000000D2	00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75 00 FB B8 00 BB CD 1A
000000E7	66 23 C0 75 3B 66 81 FB 54 43 50 41 75 32 81 F9 02 01 72 2C 66
000000FC	68 07 BB 00 00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66 53
00000111	66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66 61 68 00 00 07 CD
00000126	1A 5A 32 F6 EA 00 7C 00 00 CD 18 A0 B7 07 EB 08 A0 B6 07 EB 03
0000013B	A0 B5 07 32 E4 05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD
00000150	10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8 24 02 C3 49 6E
00000165	76 61 6C 69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61 62 6C 65
0000017A	00 45 72 72 6F 72 20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74
0000018F	69 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E 67 20 6F 70
000001A4	65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 00 00 00 63 7B 9A E2
000001B9	FC 0E D5 01 01 80 20 21 00 07 FE FF FF 00 08 00 00 00 D0 5C 0C

Figure 2: Bootstrap Code Area in Hex

• Partition Table:

The partition table is investigated to find the available partitions, find the bootable and active partitions and to specify if any extended partition is available. First, to locate the partition table, we need to read between the offsets that

compose the partition table starting from 1BE (446) and ending with 1FD (509). Using Hex Workshop, the four partition tables are located as the shown in Figure 3:

000001B9	FC 0E D5 01 01 80 20 21 00 07 FE FF FF 00 08 00 00 00 D0 5C 0C
000001CE	00 FE FF FF 07 FE FF FF 00 D8 5C 0C 00 90 01 00 00 FE FF FF 00
000001E3	FF FF FF 00 68 5E 00 00 80 01 00 00 00 00 00 00 00 00 00 00 00
000001F8	00 00 00 00 00 00 55 AA

Figure 3: Partition Table Entries in Hex

Based on the result extracted from Hex Workshop tool, only one active partition is found that is partition #1. As shown in Figure 3, the active partition starts with the value (80h) which indicate to standard active partition in the MBR sector. The other partitions are considered as non-active partition since are starting with the value (00). This indicates that only one bootable partition is available to continue booting process.

Based on the given result, only one partition will be analyzed that is the active partition. Each hexadecimal value in this active partition will be examined to extract the required information like starting and ending sectors in CHS values, the file system and the size of the partition. The partition is 16-bytes in length as shown in Figure 4 that will be examined depending on the MBR partition table structure.

000000196	74 65 6D 00 4D 69 73 73 69 6E 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 00
0000001B3	00 00 63 7B 9A E2 FC 0E D5 01 01 80 20 21 00 07 FE FF FF 00 08 00 00 00 D0 5C 0C 00 FE
0000001D0	FF FF 07 FE FF FF 00 D8 5C 0C 00 90 01 00 00 FE FF FF 0C FE FF FF 00 68 5E 0C 00 88 01
0000001ED	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA

Figure 4: Active Partition in Hex

The 16-byte partition table entry is distributed among six contents of the active partition with different length of bytes. For more clarification, this structure is described in the

following table that provides the results of Active partition analysis:



Table 2. Active Partition Analyzing Results

Contents	Relative Offsets	Length in bytes	Description
Boot Indicator	0 (80)	1	- Indication of the active partition that guide the boot loader to the required partition to boot. - Referred as SYSTEM partition in Windows OS.
Starting CHS values	1 -3 (20 21 00)	3	- Indicates the starting sector of the partition in Cylinder Head Sector values. - In hex, are read in reverse case as 00 21 20 .
Partition type (File System)	4 (07)	1	- Representation of the partition's file system - Also, it can be referred to as Partition ID - It specifies the file system used by the partition and represents the access method to the partition. - The value (07) indicates to NTFS file system that is supported in Microsoft Windows and Microsoft DOS.
Ending CHS values	5 – 7 (FE FF FF)	3	- Indicates the ending sector of the partition in Cylinder Head Sector values. - As mentioned in the starting sector, the values are read as FF FF FE in hex.
Starting Sector	8 -11 (00 08 00 00)	4	- It indicates the starting sector of the active partition. - Read in hex as 00 00 08 00 . - Represented in decimal as 2048
Partition Size	12 – 15 (00 D0 5C 0C)	4	- Represents partition size in sectors. - It is read as 0C 5C D0 00 in hex. - The size in sectors is 207409152 sectors (decimal). - The size in bytes is: - 106193485824 Bytes = 101274 MiB = 98.9 GiB

As mentioned in the above table, the used file system is NTFS. The partition start at sector 2048 and the size of the partition is 98.9 Gigabytes.

• **Boot Record Signature**

Locating the Boot record signature or the magic number requires searching in the offsets 1FE and 1FF that represent the 2-byte value as (55AA) in hex as shown in Figure 5.

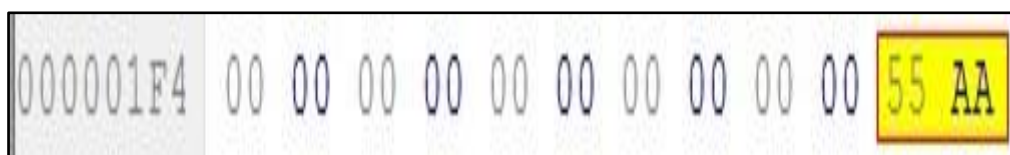


Figure 4: Boot Record Signature in Hex

Most required information is extracted easily from the MBR since it has a standard structure followed by most computer machines. In this research, only one active partition is analyzed to clarify the basic structure of the MBR and to extract the required disk information for forensic investigations.

4. CONCLUSION

MBR is an essential part in the computer that is physically located in the first sector of the disk and controls the booting process in the computer. As presented in this research, all MBR patterns are located in standard locations in the first sector. Therefore, studying its structure is required to make sure that the computer is not infected by malicious programs like malware that may replace the MBR and load malicious software to the computer memory during booting process. Moreover, this helps forensic investigators to extract disk

partition details like the file system type used by the portion and the disk partition size. Further research might be required in the future to study the vulnerabilities exploited by malicious programs to infect the MBR and get control over booting process.

5. REFERENCES

[1] R. G. Minnich, "Operating System," 2004.
 [2] Microsoft, "Windows support for hard disks that are larger than 2 TB," 2013. [Online]. Available: <http://support.microsoft.com/kb/2581408#appliesto>.
 [3] P. ARNTZ, "Meet the Master Boot Record," 2014. [Online]. Available: <https://blog.malwarebytes.org/security-threat/2014/09/meet-the-master-boot-record/>.



- [4] M. TechNet, “Master Boot Record,” 2011. [Online]. Available:<http://technet.microsoft.com/enus/library/cc976786.aspx>.
- [5] M. TechNet, “Disk Concepts and Troubleshooting,” 2011.[Online].Available:<http://technet.microsoft.com/enus/library/cc977219.aspx>.
- [6] J. Gu and W. Ji, “A secure bootstrap based on trusted computing,” Proc. - 2009 Int. Conf. New Trends Inf. Serv. Sci. NISS 2009, no. 3, pp. 502–504, 2009.
- [7] R. McKemmish, “What is forensic computing?,” Trends Issues Crime Crim. Justice, vol. 118, no. 118, pp. 1–6, 1999.