## 作业3 自学RAID5数据恢复技

**姓名**： 黄鑫

**学号**： 20210509010

**日期**： 5.19

注意：提交文档的命名规范：作业3+姓名+学号.doc

### 学习目标：

磁盘阵列的结构

RAID5数据恢复分析方法

### 资源：

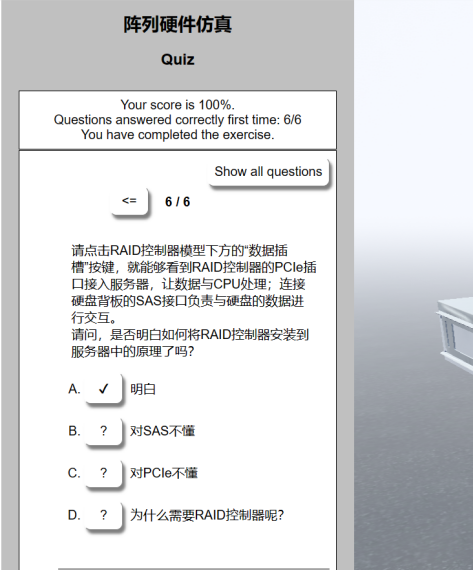
http://121.48.165.7:8080/

RAID虚拟.zip

WinHex

### 了解RAID 服务器结构

学习“http://121.48.165.7:8080/” – “基础知识” – “阵列硬件仿真”，完成左窗口的问答题，截图。



### 了解RAID5数据恢复分析方法

1. 根据“http://121.48.165.7:8080/” – “基础知识” – “磁盘阵列概述” 和课件“数据7-数据恢复技术”的p79~p88页，了解RAID 5 的组成结构，理解磁盘阵列中“条带”的作用、“校验块/盘”的作用。

**“条带”的作用：**

提高性能：条带化允许RAID 5并行读取和写入数据，因此可以提高数据访问的速度。通过将数据分成块并同时在多个磁盘上存储，可以有效地增加数据传输速率。

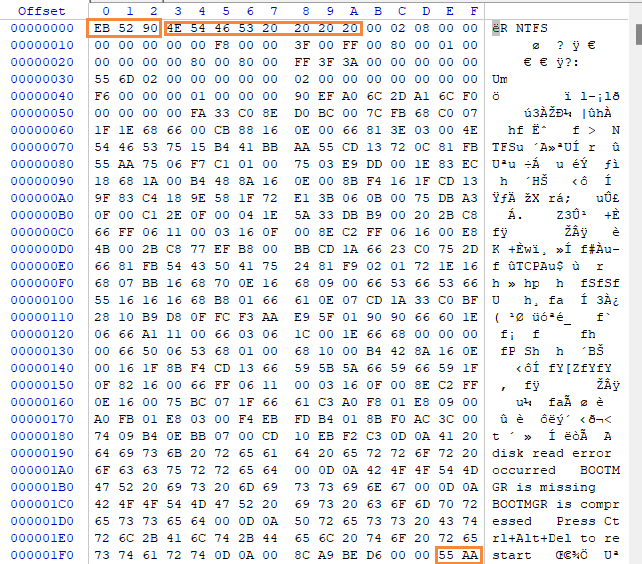
均衡负载：条带化还有助于均衡系统负载，因为数据被均匀地分布在多个磁盘上。这意味着每个磁盘都可以参与数据访问和传输，从而减轻了单个磁盘的压力。

**“奇偶校验块/盘”的作用：**

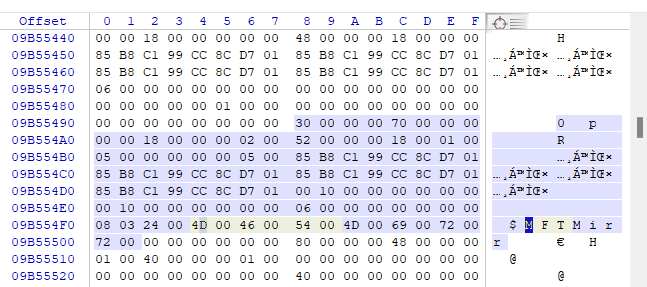
数据恢复：奇偶校验信息允许RAID 5在发生磁盘故障时恢复丢失的数据。通过奇偶校验计算，RAID 5可以计算出丢失数据的值，并将其恢复到另一个磁盘上。

容错性：即使一个数据盘失败，RAID 5仍然可以继续正常运行。当某个数据盘出现故障时，RAID 5可以使用奇偶校验信息来恢复丢失的数据，从而保持数据的完整性和可用性。

1. 根据“http://121.48.165.7:8080/” – “RAID恢复” – “RAID 5”的问答指导，在本机上使用WinHex完成对“**RAID虚拟.zip**”的分析和数据恢复。（RAID虚拟.zip 解压后有5个磁盘镜像文件）
2. 载入后，查看第1个扇区（即0号扇区）：第1，2，3个字节为"EB 52 90"，这是MBR的跳转指令。第4、5、6、7字节为“4E 54 46 53 20”，ASCII码为“NTFS”。该扇区的最后两个字节为“55 AA”。**由此NTFS的$BOOT文件就是DBR，是NFTS分区的起始扇区。这里可以确定该磁盘是RAID保存数据的第1个磁盘**。



1. 通过$BOOT扇区，可以获得:$MFT的起始簇号为159,061；每个簇由8个扇区组成；因此$MFT的逻辑起始扇区号为1272488，换算为字节1,272,488 x 512 = 651,513,856B，$MFT开始的位置大约在651,513,856/4 = 162,878,464 字节处，即9B5 5400，在2.dd、3.dd、4.dd和5.dd的9B5 5400字节的位置寻找46 49 4C 45（即FILE），在2.dd中找到。



（3）找到$MFT之后，就可以开始分析RAID5的结构了。  
我们在3.dd的9B5 5400字节的位置开始，偏移44个字节的位置，确定文件记录号为01H（1）；  
我们在3.dd的9B5 5400 + 44字节的位置发现这个$MFT的文件记录号为41H（65）；  
我们在4.dd的9B5 5400 + 44字节的位置发现这个$MFT的文件记录号为81H（129）；  
我们在5.dd的9B5 5400 的位置确定是乱码，判断是该位置是条带的校验值；  
这样可以判断磁盘的条带大小是，RAID5的条带估计有几个文件记录大，因此将不同磁盘相邻的文件记录号相减，最小的差值就是条带的大小。 129-65 = 64， 64 -1 = 64 因此条带大小为64个文件记录，将1.dd 2.dd 3.dd 4.dd四个磁盘09B5540H开始的四个字节异或，等于B9 B6 B3 BA，与5.dd的四个字节一致。



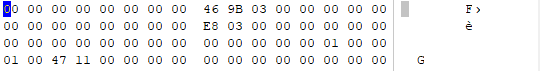
（4）加载2.dd，从$MFT的文件记录1开始跳到128号扇区，即65536（10000H）个字节。该文件记录的ID号是141h

1.dd 101H, 257

  
2.dd 141H, 321

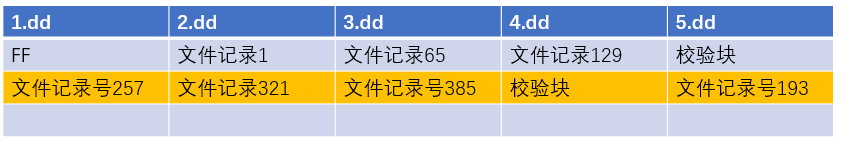
  
3.dd 181H, 385

  
4.dd 校验块

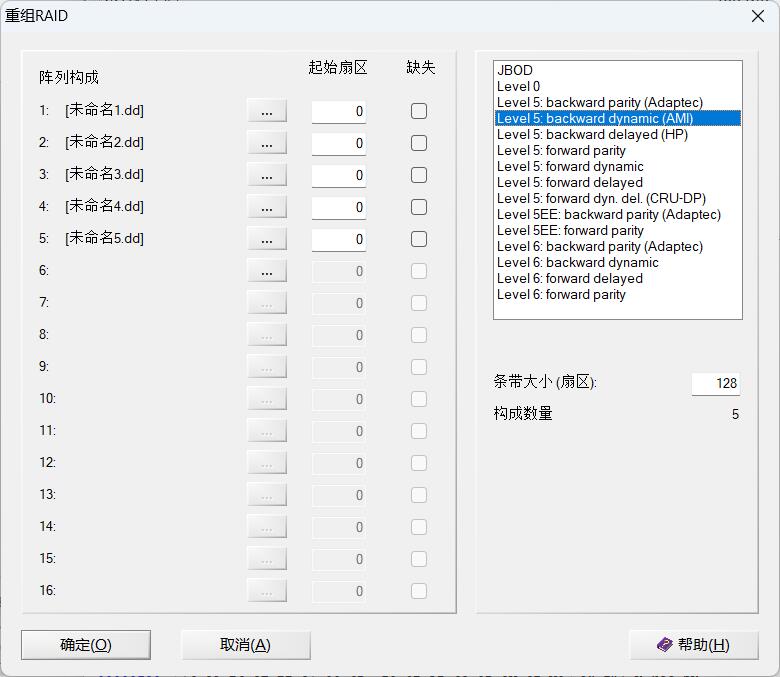
  
5.dd C1H 193

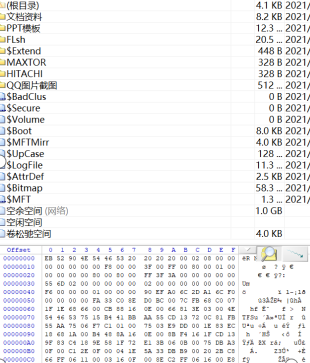


(5)分析可得，左同步

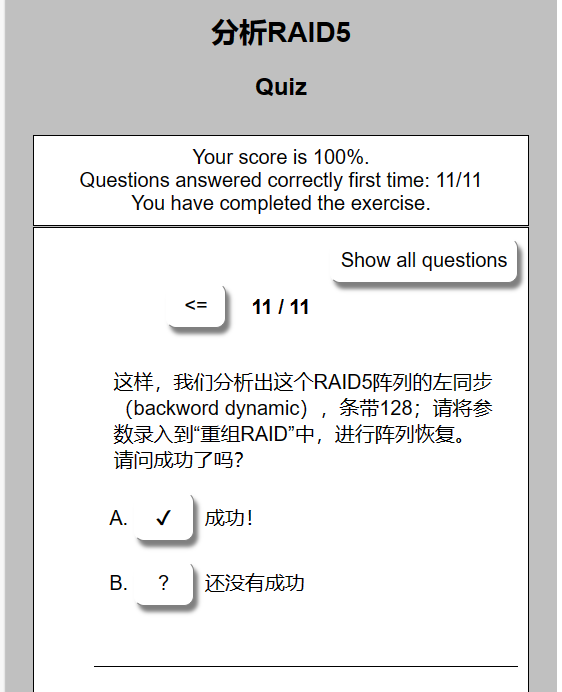


1. 进行重组，得到结果





1. 完成左窗口“RAID 5”的问答指导的问答题，截图。



### 问答：

若一个RAID5磁盘阵列，采用的是NTFS文件系统：

1. 如何确定$MFT起始位置在哪个硬盘？

首先，通过读取$BOOT扇区，可以获取到$MFT的起始簇号以及每个簇的扇区数。这样可以计算出$MFT的逻辑起始扇区号。

其次，根据组成RAID5磁盘阵列的磁盘数量，可以推算出$MFT在整个磁盘阵列中的可能位置。然后在每个磁盘上对应的位置搜索特定的文件标识，如46 49 4C 45（即"FILE"）。

最后，检查找到的位置是否有30H属性，如果是$MFTMirr属性，则表明该位置是$MFT的起始位置。

1. 如何根据NTFS文件记录确定磁盘阵列条带大小？还有什么方法可以确定磁盘阵列条带大小？

通过分析NTFS文件记录在磁盘上的分布情况，可以推断出条带大小。例如，如果文件记录跨越多个物理硬盘，并且在每个硬盘上都具有相同的偏移量，那么可以推测条带大小等于相邻记录号之差。

另一种方法是，在一个物理盘中找到一个校验条带的开始扇区，并记住这个扇区号。然后继续向后查找，直到突然出现了正常的数据。这表明校验条带已经结束。此时校验条带的开始扇区到正常数据所在扇区之间的扇区数，即为一个条带的大小。