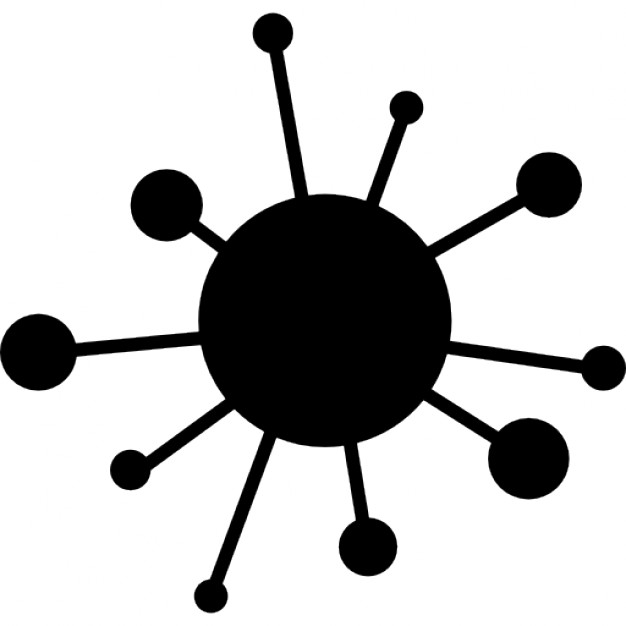
# 计算机病毒学

论述题



学号：0x091395

姓名：uknowho

论述题

根据课堂讲授的基于FAT32、NTFS文件系统的WINDOWS XP启动过程分析，回答以下问题：（20分）

1. WINDOWS XP在FAT32文件系统中寻找根目录的过程是怎样的？

FAT32文件系统结构如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| DBR及保留扇区 | FAT1 | FAT2 | DATA区 |

数据区起始扇区号=分区起始扇区+DBR及保留扇区+（FAT表\*2）；

根目录位置=数据区扇区+簇大小\*2

参考：http://dengqi.blog.51cto.com/5685776/1349327

1. WINDOWS XP在NTFS文件系统中寻找根目录的过程是怎样的？

根目录=分区起始地址+$MFT起始簇号\*每簇扇区数+2\*5

参考：http://dengqi.blog.51cto.com/5685776/1351300

1. WINDOWS XP在FAT32文件系统中读取NTLDR系统启动文件的过程是怎样的？

操作系统为了管理磁盘上的目录和文件，在特定的扇区上建立了一个文件目录表FDT

NTLDR=在根目录中遍历FDT，查找NTLDR

1. WINDOWS XP在NTFS文件系统中读取NTLDR系统启动文件的过程是怎样的？

定位到根目录后找到索引区域所在的簇，遍历每一个索引项，查找NTLDR文件

1. WINDOWS XP在FAT32文件系统中要保证文件数据的安全是怎样做的？

FDT中有删除标志位，若要删除某一文件，修改其标志位为已删除（E5），且把数据所在簇设置为空闲簇。但文件实际并未删除。可以修改其删除位，在某种程度上达成恢复数据的办法。

1. WINDOWS XP在NTFS文件系统中要保证文件数据的安全是怎样做的？

$MFT的14H,15H设置为00，系统判定为已删除。恢复文件只要找到文件所在起始扇区号即可。  
且NTFS提供数据加密功能，也可以在一定程度上保证数据安全

1. 你在写引导型病毒时，想同时具备感染FAT32和NTFS文件系统的功能，你该怎么设计你的感染程序？

把病毒代码写到引导记录之前，或者在固定地址启动跳转指令之后，跳转到病毒代码处，等待病毒代码执行完之后，继续执行原先的引导程序

1. 你在设计小型操作系统时，会选择FAT32和NTFS文件系统中的哪一个？理由是什么？你会根据这些知识，自己设计一个文件系统吗？说说你的理由。

选择NTFS

安全性高：NTFS支持基于文件或目录的ACL，并且支持加密文件系统（EFS）。

可恢复性：NTFS支持基于原子事务概念的文件恢复，比较符合服务器文件系统的要求。

文件压缩：NTFS支持基于文件或目录的文件压缩，可以很方便的节省磁盘空间。

磁盘配额：NTFS支持磁盘配额，可针对系统中每个用户分配磁盘资源。

文件索引：采用索引方式，搜索文件速度高。

能力强的话，应该会设计一个玩一下~