

# 加密工具的使用体验

- xiabee

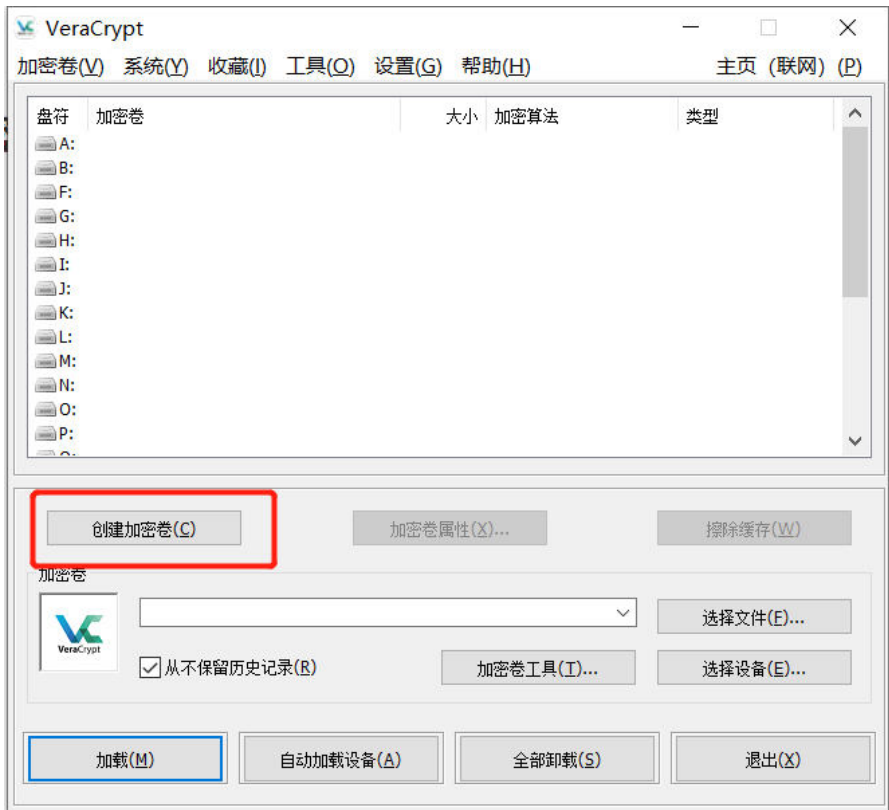
## 一、实验步骤

- 使用 Veracrypt 创建加密卷，并将加密卷保存在U盘上；
- 再使用 BitLocker 对u盘进行加密；

## 二、实验过程

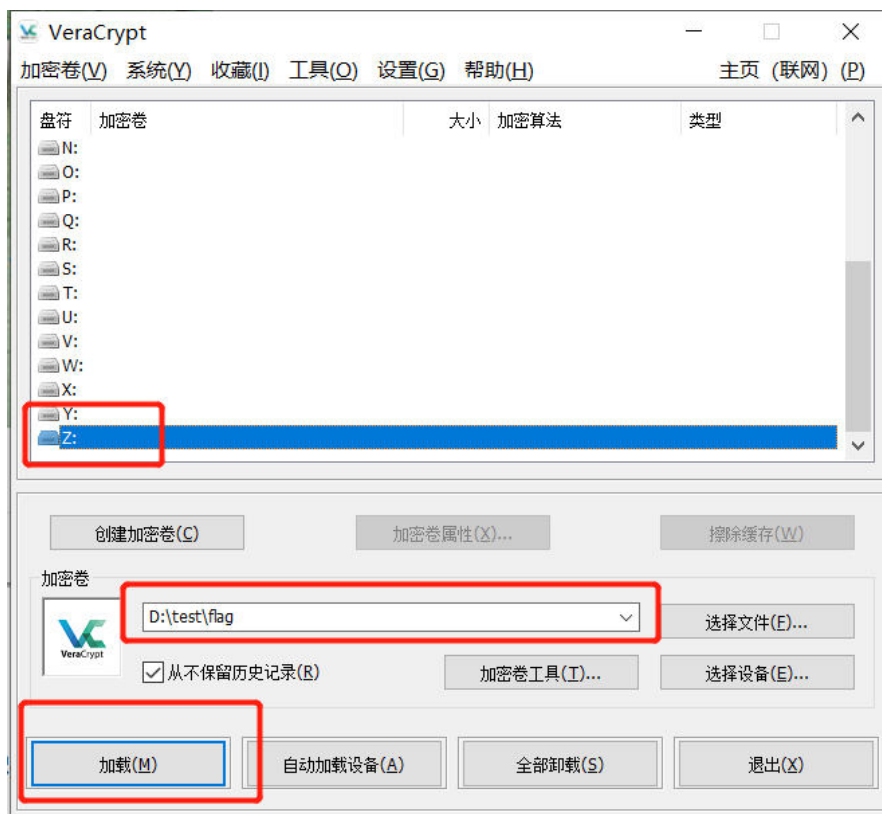
### 0x01 VeraCrypt 创建加密分区

- 创建加密卷

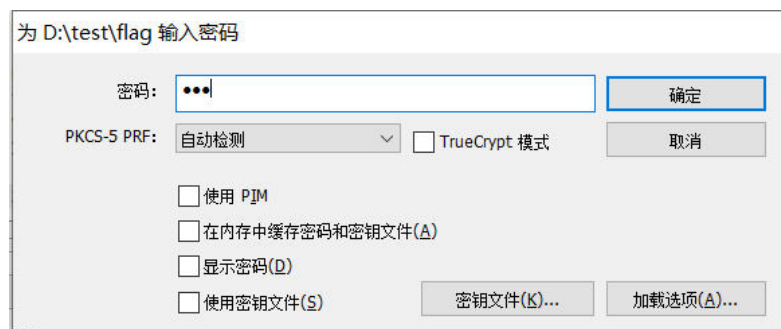


- 创建文件类型加密卷——标准的VeraCrypt加密卷——选择加密卷位置——设置加密算法和哈希算法





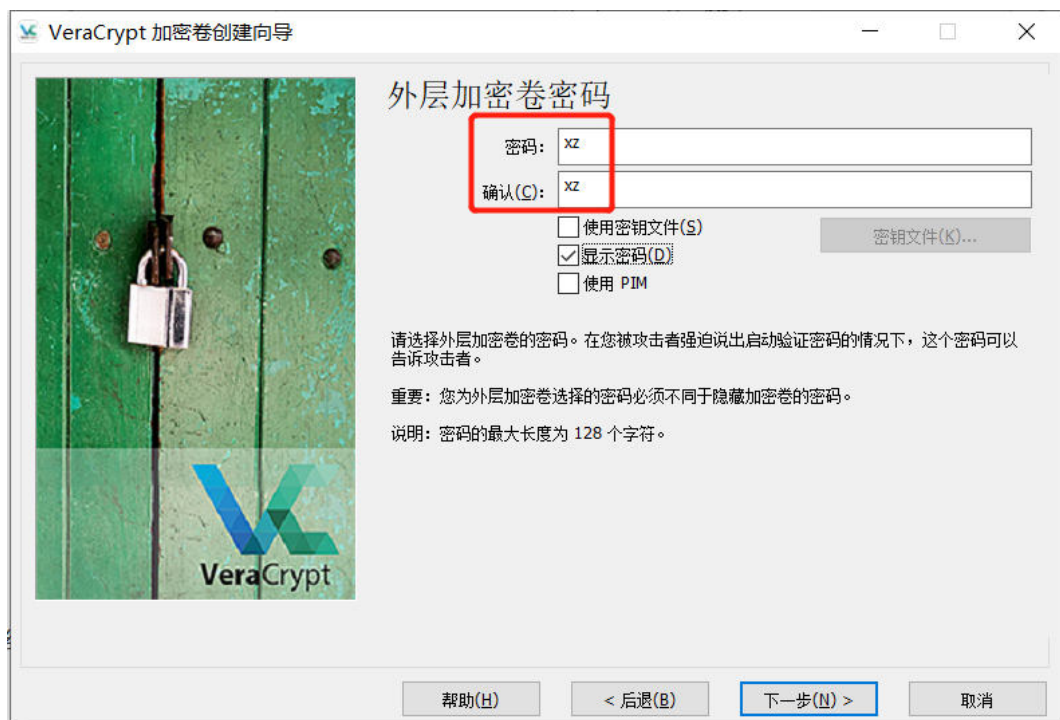
- 输入密码



此时可以看到，"Z"盘已经成功挂载

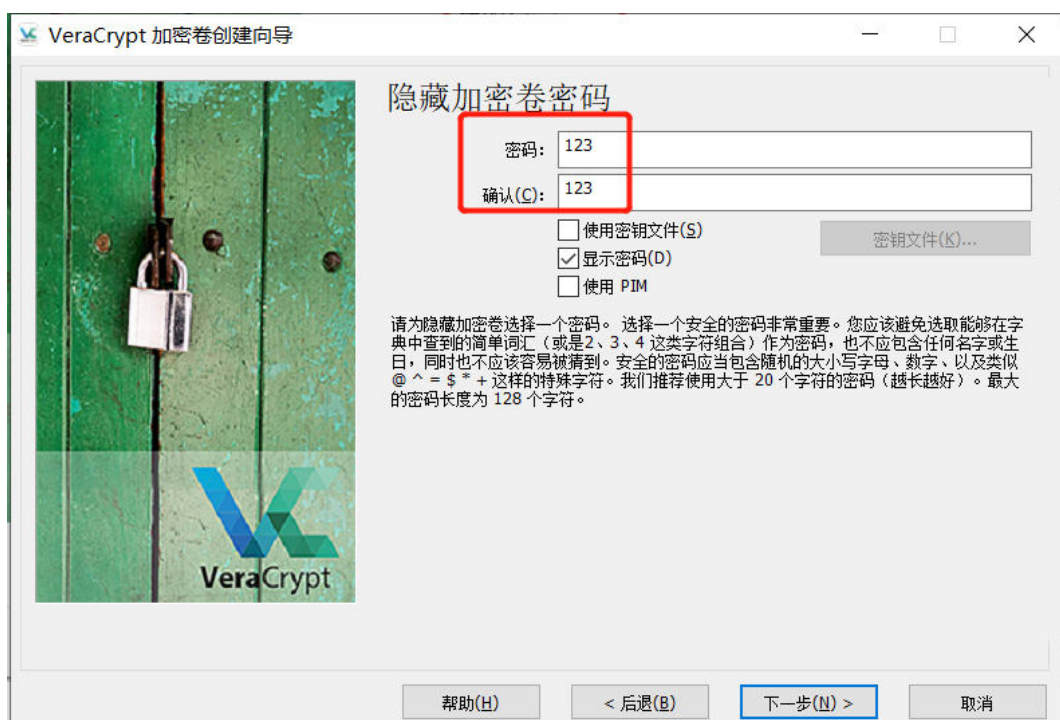
## 0x03 VeraCrypt 创建隐藏加密卷

- 创建文件型加密卷——隐藏的VeraCrypt加密卷——常规模式——外层加密卷，命名为 FLAG.ISO



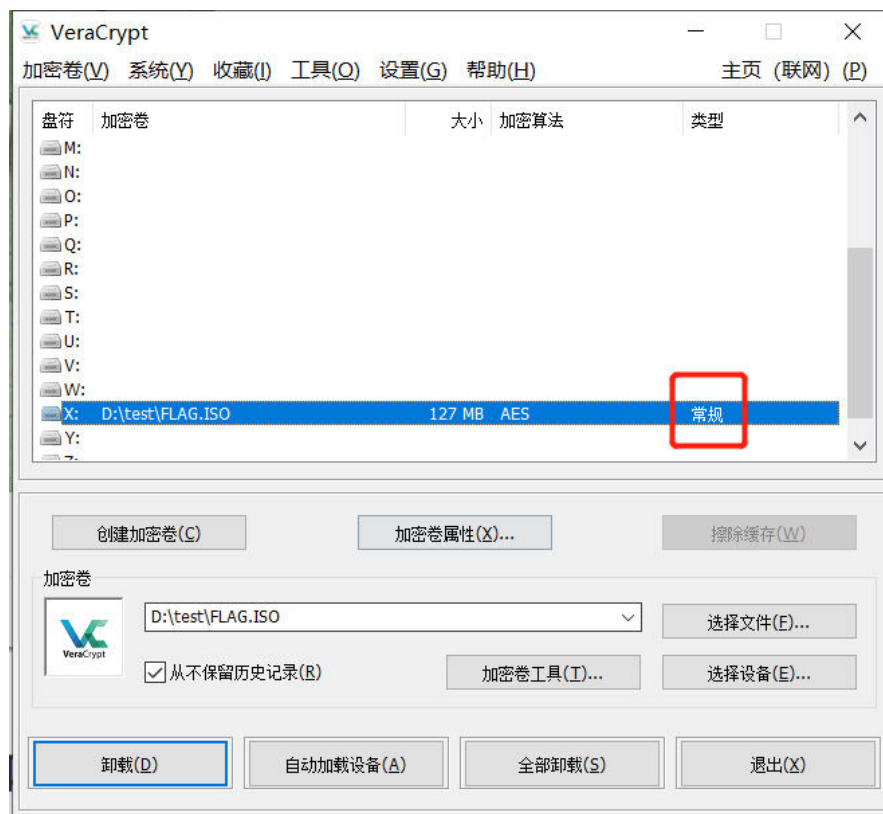
外层加密卷密码为 xz

- 设置隐藏加密卷密码，不能与外层加密卷密码相同



## 0x04 VeraCrypt 读取隐藏加密卷

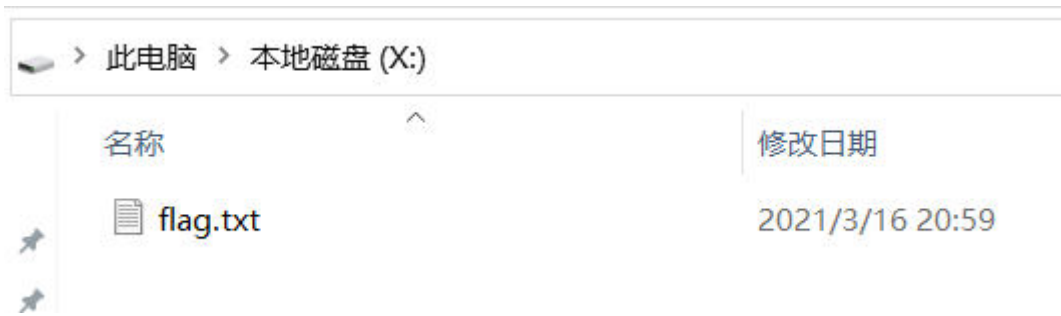
- 输入外层加密卷密码 xz，得到常规加密卷：



此时只有一个文件 `fake_flag.txt`

- 输入隐藏加密密码 123，得到隐藏加密卷：





此时有另一个文件 flag.txt

## 0x05 创建文件保险柜

- 将刚刚的 FLAG.ISO 拷贝至U盘中



此时的 FLAG.ISO 便是我们的文件保险柜

- 使用 file 命令查看文件类型:



仅能查看到为数据类型文件，无法看到详细内容

## 0x06 BitLocker加密整个U盘

可移动数据驱动器 - BitLocker To Go

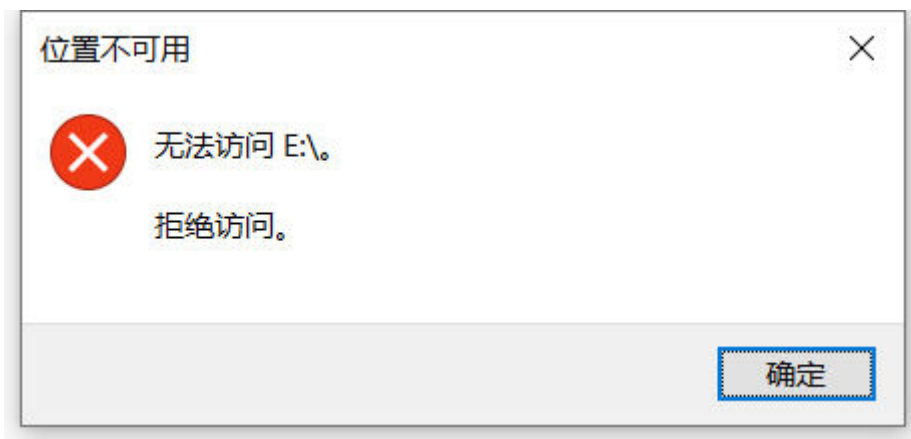
64 GB (E:) BitLocker 已启用



备份恢复密钥  
更改密码  
删除密码  
添加智能卡  
启用自动解锁  
关闭 BitLocker

此时直接访问U盘会提示不可访问:





从“此电脑”中访问，提示输入密码：



解锁后成功访问：



### 三、实验心得

- 创建加密文件卷很容易，给文件加密也比较简单；但是某些特定时候被迫交出加密密钥，这时隐藏加密卷的优势就显得十分明显
- VeraCrypt 加密的文件需要特定工具（如 VeraCrypt 本身）才能打开，使用不是很方便；可以通过逆向工程对U盘本身引导头进行改写，摆脱对工具的依赖