工控安全异常取证分析

2021-09-01 | Challenge， 2021， 工业信息安全技能大赛， 线上赛-第一场

Challenge | 2021 | 工业信息安全技能大赛 | 线上赛-第一场 | 工控安全异常取证分析

点击此处获得更好的阅读体验

WriteUp来源

来自 Venom 战队

题目描述

> 网络安全人员小吕在工厂中发现某台工程师站主机可能感染了病毒，小吕将磁盘导出后请你能帮忙一起分析出异常。flag格式为：flag{}

题目考点

- 磁盘数据取证

解题思路

解压出来两个文件，一个1122，文件挺大，另一个是 112233只有1KB，一看就知道是个vmdk。

打开112233，找到其真实名称

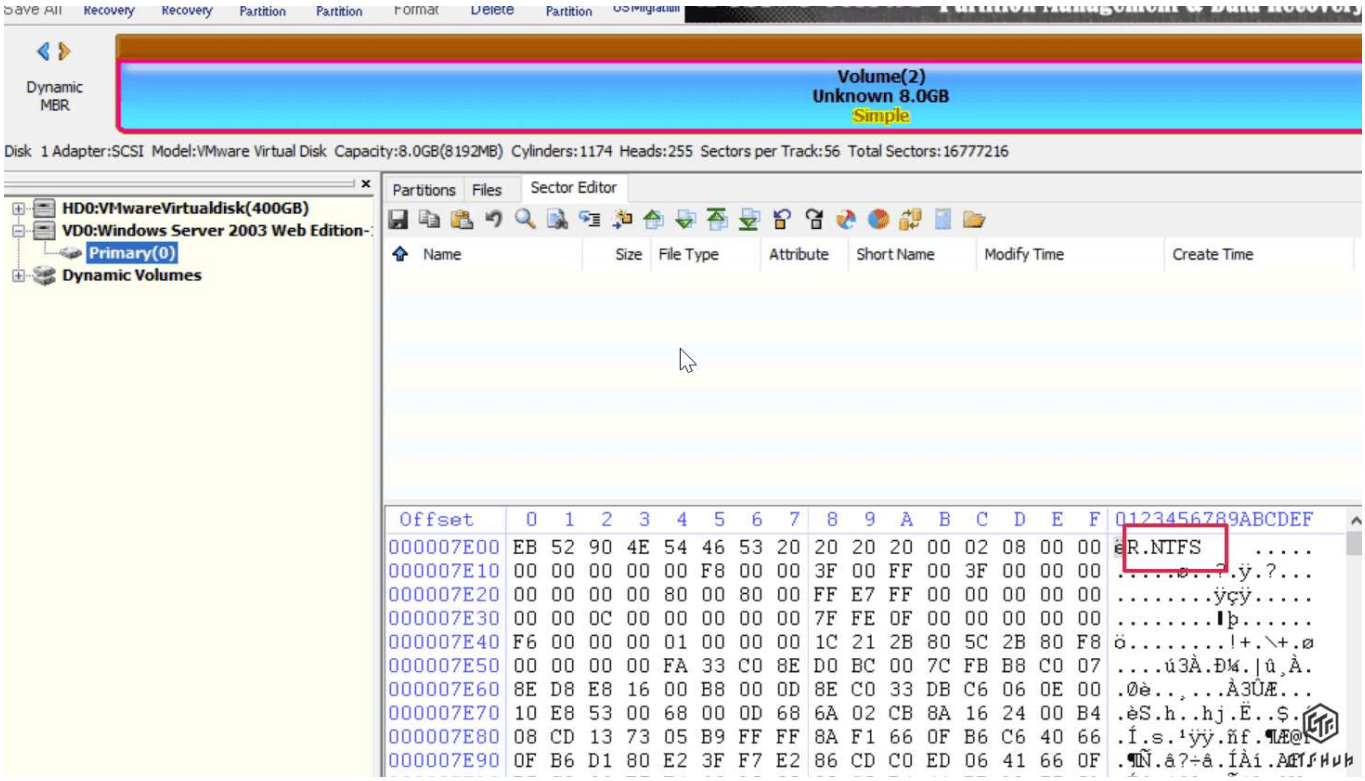
112233

```
# Disk DescriptorFile
version=1
encoding="GBK"
CID=4e115737
parentCID=ffffffff
createType="monolithicFlat"

# Extent description
RW 16777216 FLAT "Windows Server 2003 Web Edition-1-flat.vmdk" 0

# The Disk Data Base
#DDB

ddb.adapterType = "lsilogic"
ddb.geometry.cylinders = "1174"
ddb.geometry.heads = "255"
ddb.geometry.sectors = "56"
ddb.longContentID = "6adfeb870f7413841576eb994e115737"
ddb.uuid = "60 00 C2 9d 19 e5 98 5e-b2 70 16 69 7d b0 d6 f0"
ddb.virtualHWVersion = "16"

```

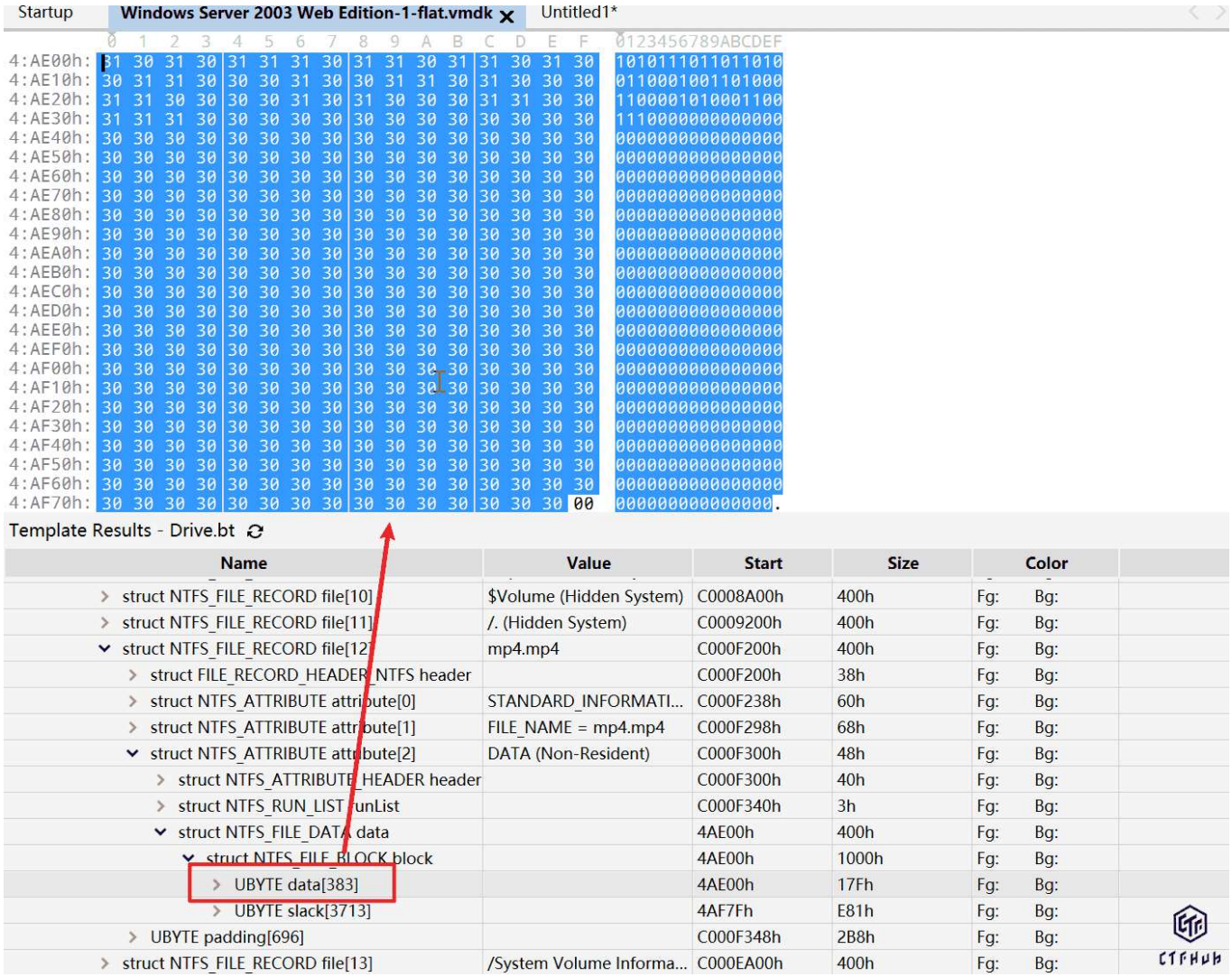
将 `112233` 改名为 `Windows Server 2003 Web Edition-1.vmdk`

将 `1122` 改名为 `Windows Server 2003 Web Edition-1-flat.vmdk`

用 `DiskGenius` 打开，应该是个NTFS分区FDD，没有分区表的那种。



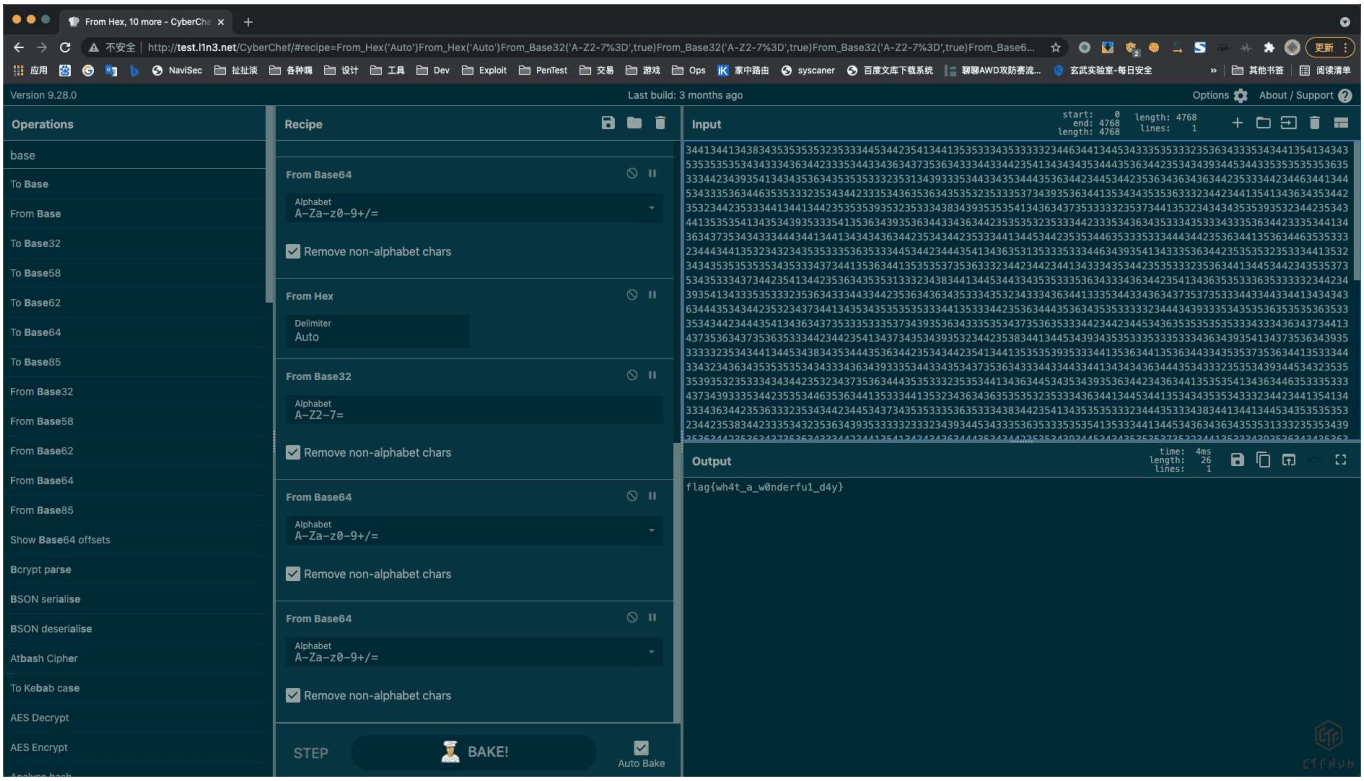
从名为 mp4.mp4 的文件中提取出一段 ascii 字符串



提取出字符串

```
1  3441344134383435353535323533344534423541344135353334353333323446344134453433353533
```

之后 按照如下顺序进行解码即可得到flag，HEX -> HEX -> B32 -> B32 -> B32 -> B64 -> B64 -> HEX -> B32 -> B64 -> B64



Flag

```
1  flag{wh4t_a_w0nderfu1_d4y}
```


Challenge # 2021 # 工业信息安全技能大赛 # 线上赛-第一场

隐藏的工程 异常的梯形图分析