CTF之隐写术总结

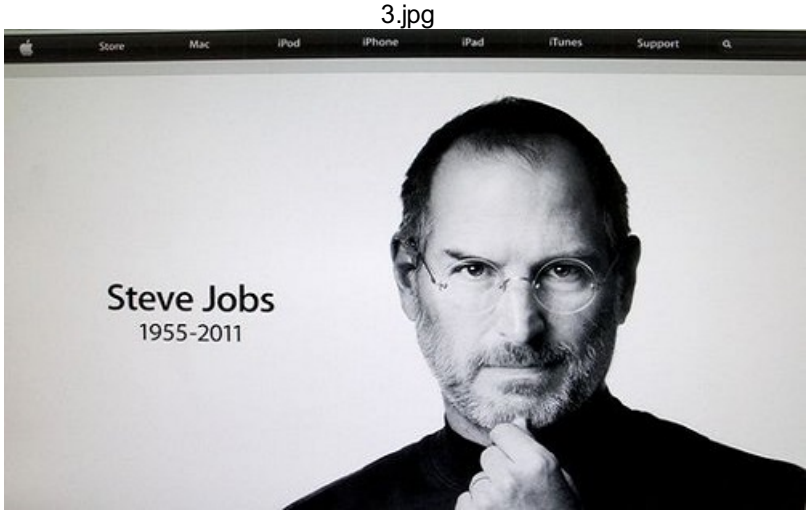
原创

ntkkjjh 于 2017-10-20 22:16:01 发布
分类专栏： 渗透测试 文章标签： CTF

一、图片隐写

1.cmd命令行copy /b 1.jpg+2.jpg 3.jgp 以二进制方式连接两个图片，正常的jpg文件结束标志是FF D9，因此只会显示1.jgp，下图是合成的3.jpg。

3.jpg



2.使用binwalk工具分析图片，分析结果（windows下先安装binwalk：python setup.py install）：

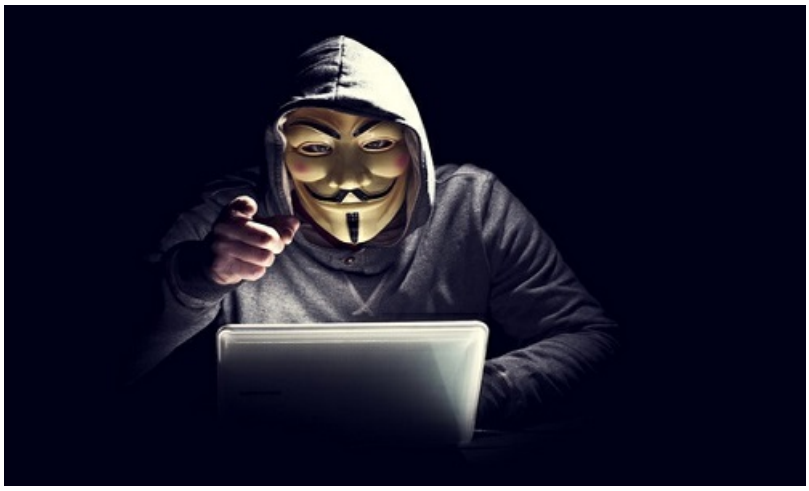
```
C:\Python27\Scripts>python binwalk 3.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

0             0x0             JPEG image data, JFIF standard 1.01
35786         0x8BCA          JPEG image data, JFIF standard 1.01
35816         0x8BE8          TIFF image data, big-endian, offset of first image
```

可以发现从35786块偏移开始有另一张jpg图片

3.使用WinHex工具分离图片：

jpg格式文件开始的2字节是FF D8，之后2个字节是FF E0 ，最后2个字节是图像文件结束标记为FF D9 。我们打

2.jpg



4.linux下使用dd命令：

```
dd if=3.jpg of=2.jpg skip=35786 bs=1
```

可以参考dd命令详解，这里if是指定输入文件，of是指定输出文件，skip是指定从输入文件开头跳过35786个块后再开始复制，bs设置每次读写块的大小为1字节 ，得到隐藏图片2.jpg。

5.使用foremost工具分离:

foremost是一个基于文件文件头和尾部信息以及文件的内建数据结构恢复文件的命令行工具，win可以下载地址，Linux可以通过下面命令安装使用：

```
apt-get install foremost
```

安装foremost后你可以使用foremost -help查看使用帮助，这里最简单分离文件的命令为：

```
foremost 3.jpg
```

当我们使用这行命令后，foremost会自动生成output目录存放分离出文件。

待续。。。。