专注APT攻击与防御
https://micropoor.blogspot.com/

Exiftool简介：

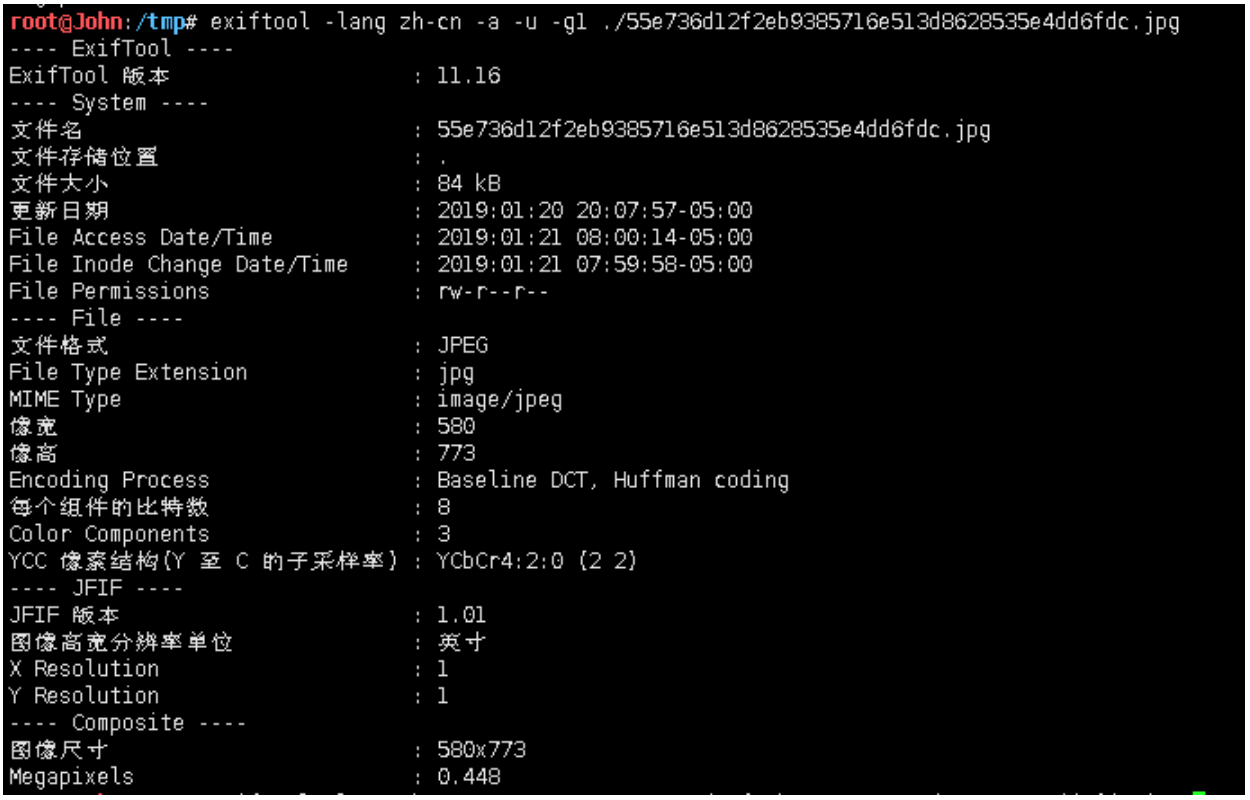
ExifTool可读写及处理图像、视频及音频，例如Exif、IPTC、XMP、JFIF、GeoTIFF、ICC Profile。包括许多相机的制造商信息读取，如佳能，卡西欧，大疆，FLIR，三星等。

同样它支持多国语言


```
root@John:/tmp# exiftool -lang zh-cn -a -u -g1 ./55e736d12f2eb9385716e513d8628535e4dd6fdc.jpg
---- ExifTool ----
ExifTool 版本 : 11.16
---- System ----
文件名 : 55e736d12f2eb9385716e513d8628535e4dd6fdc.jpg
文件存储位置 : .
文件大小 : 84 kB
更新日期 : 2019:01:20 20:07:57-05:00
File Access Date/Time : 2019:01:21 08:00:14-05:00
File Inode Change Date/Time : 2019:01:21 07:59:58-05:00
File Permissions : rw-r--r--
---- File ----
文件格式 : JPEG
File Type Extension : jpg
```

```
MIME Type : image/jpeg
像宽 : 580
像高 : 773
Encoding Process : Baseline DCT, Huffman coding
每个组件的比特数 : 8
Color Components : 3
YCC 像素结构(Y 至 C 的子采样率) : YCbCr4:2:0 (2 2)
---- JFIF ----
JFIF 版本 : 1.01
图像高宽分辨率单位 : 英寸
X Resolution : 1
Y Resolution : 1
---- Composite ----
图像尺寸 : 580x773
Megapixels : 0.448

```



在大型内网渗透中，尤其是针对办公机的渗透，需要熟知目标集体或者个人的作息时间，工作时间，文档时间，咖啡时间，或者需要从某些文件中获取对方的真实拍摄地坐标等。那么无疑需要快速的从大量文件中筛选信息诉求。当目标越复杂，文件中的信息搜集就更为重要。如文档作者，技术文章作者，财务文档作者等，熟知在大量人员，获取对方职务，大大减少渗透过程中的无用性，重复性，可见性。与暴露性。而作为公司，应该熟悉相

关文档的内置属性，尤其是在共享文件服务器上，删除或者复写敏感信息来降低企业安全风险。本篇意旨企业安全在处理本公司相关敏感文件以及重要文件应做好更多的防范，尤其是重要部门，如研发，财务等。

- Micropoor