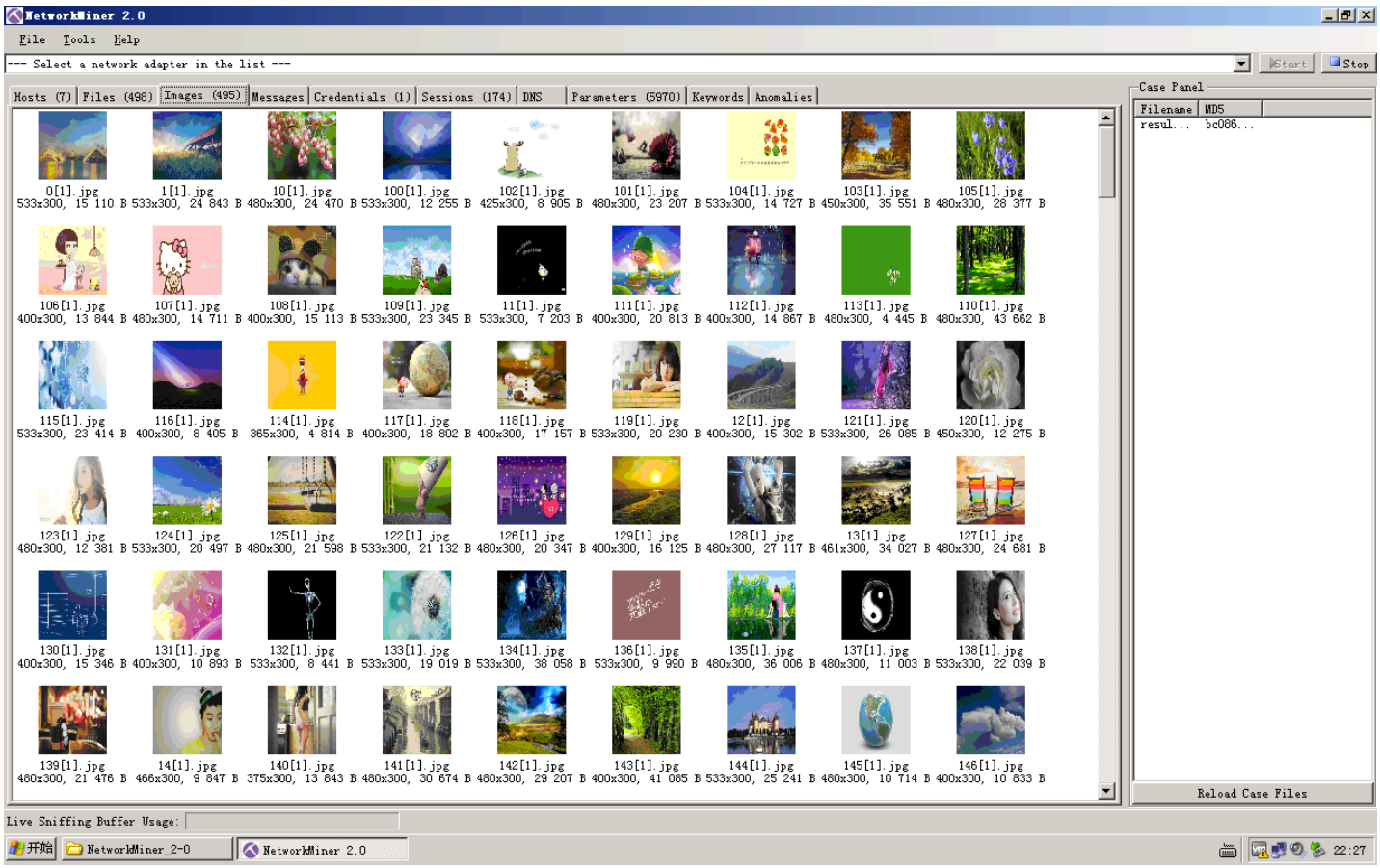
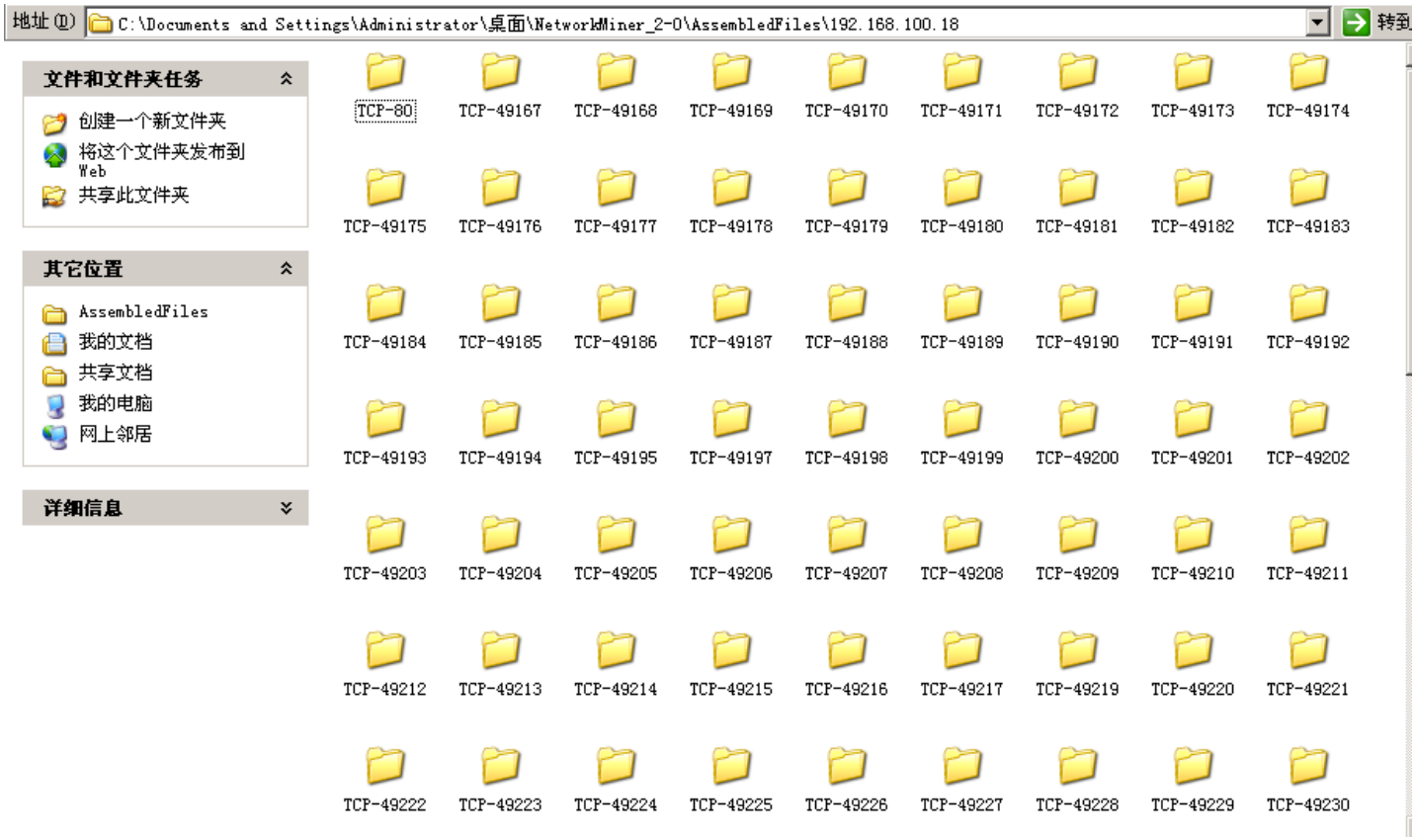
MISC3

1) 使用NetWorkMiner提取FTP流量中的图片

提取图片使用的是[NetWorkMiner](),可以直接将PCAP文件中的图片提取出来。



提取出的照片的文件位置在NetWorkMiner目录下的 **AssembledFiles**下



照片分两种情况：

1、从HTTP流量提取出的（文件夹TCP－80）

2、从FTP流量提取出的（剩余其他的都是FTP的）

对于获取从HTTP流量中提取的jpg的exif信息，测试了好多次，用**NetWorkMiner**提取的图片获取不到flag信息，不过，从**WireShark**中提取的图片可以获取到。

2) 使用WireShark提取HTTP流量中的图片

使用WireShark加载PCAP文件，按照下面操作将jpg图片提取出来:

[File] ---> [Export Obiects] ---> [HTTP]

```
[root@Kali20:~/Downloads/MISC3/all-jpg# ls                                                                ]
0(1).jpg    116(2).jpg  149.jpg    2(1).jpg    37.jpg      53(2).jpg  6.jpg       85.jpg
0(2).jpg    116.jpg     14.jpg     21.jpg      38(1).jpg   53.jpg     70(1).jpg   86(1).jpg
0.jpg       117(1).jpg  150.jpg    22(1).jpg   38(2).jpg   54(1).jpg  70(2).jpg   86(2).jpg
100(1).jpg  117(2).jpg  15(1).jpg  22(2).jpg   38.jpg      54(2).jpg  70.jpg      86.jpg
100(2).jpg  117.jpg     151.jpg    2(2).jpg    39(1).jpg   54.jpg     71(1).jpg   87(1).jpg
100.jpg     118(1).jpg  15(2).jpg  22.jpg      39(2).jpg   55(1).jpg  71(2).jpg   87(2).jpg
101(1).jpg  118(2).jpg  152.jpg    23(1).jpg   39.jpg      55(2).jpg  7(1).jpg    87.jpg
101(2).jpg  118.jpg     153.jpg    23(2).jpg   3.jpg       55.jpg     71.jpg      88(1).jpg
10(1).jpg   119(1).jpg  154.jpg    23.jpg      40(1).jpg   56(1).jpg  72(1).jpg   88(2).jpg
101.jpg     119(2).jpg  155.jpg    24(1).jpg   40(2).jpg   56(2).jpg  72(2).jpg   88.jpg
102(1).jpg  119.jpg     156.jpg    24(2).jpg   40.jpg      56.jpg     7(2).jpg    89(1).jpg
102(2).jpg  1(1).jpg    157.jpg    24.jpg      41(1).jpg   57(1).jpg  72.jpg      89(2).jpg
10(2).jpg   11.jpg      158.jpg    25(1).jpg   41(2).jpg   57(2).jpg  73(1).jpg   89.jpg
102.jpg     120(1).jpg  159.jpg    25(2).jpg   4(1).jpg    57.jpg     73(2).jpg   8.jpg
103(1).jpg  120.jpg     15.jpg     25.jpg      41.jpg      58(1).jpg  73.jpg      90(1).jpg
103.jpg     121(1).jpg  160.jpg    26(1).jpg   42(1).jpg   58(2).jpg  74(1).jpg   90(2).jpg
104(1).jpg  12(1).jpg   16(1).jpg   26(2).jpg   42(2).jpg   58.jpg     74(2).jpg   90.jpg
104.jpg     121.jpg     161.jpg    26.jpg      4(2).jpg    59(1).jpg  74.jpg      91(1).jpg
105(1).jpg  12(2).jpg   16(2).jpg   27(1).jpg   42.jpg      59(2).jpg  75(1).jpg   91(2).jpg
105.jpg     122.jpg     162.jpg    27(2).jpg   43(1).jpg   59.jpg     75(2).jpg   9(1).jpg
106(1).jpg  123.jpg     163.jpg    27.jpg      43(2).jpg   5.jpg      75.jpg      91.jpg
106.jpg     124.jpg     164.jpg    28(1).jpg   43.jpg      60(1).jpg  76(1).jpg   92(1).jpg
107(1).jpg  125.jpg     165.jpg    28(2).jpg   44(1).jpg   60(2).jpg  76(2).jpg   92(2).jpg
107(2).jpg  126.jpg     166.jpg    28.jpg      44(2).jpg   60.jpg     76.jpg      9(2).jpg
107.jpg     127.jpg     167.jpg    29(1).jpg   44.jpg      61(1).jpg  77(1).jpg   92.jpg
108(1).jpg  128.jpg     168.jpg    29(2).jpg   45(1).jpg   61(2).jpg  77(2).jpg   93(1).jpg
108(2).jpg  129.jpg     169.jpg    29.jpg      45(2).jpg   6(1).jpg   77.jpg      93(2).jpg
108.jpg     1(2).jpg    16.jpg     2.jpg       45.jpg      61.jpg     78(1).jpg   93.jpg
109(1).jpg  12.jpg      170.jpg    30(1).jpg   46(1).jpg   62(1).jpg  78(2).jpg   94(1).jpg
109(2).jpg  130.jpg     17(1).jpg   30(2).jpg   46(2).jpg   62(2).jpg  78.jpg      94(2).jpg
109.jpg     13(1).jpg   171.jpg    30.jpg      46.jpg      6(2).jpg   79(1).jpg   94.jpg
10.jpg      131.jpg     17(2).jpg   31(1).jpg   47(1).jpg   62.jpg     79(2).jpg   95(1).jpg
110(1).jpg  13(2).jpg   172.jpg    31(2).jpg   47(2).jpg   63(1).jpg  79.jpg      95(2).jpg
110(2).jpg  132.jpg     173.jpg    3(1).jpg    47.jpg      63(2).jpg  7.jpg       95.jpg
110.jpg     133.jpg     174.jpg    31.jpg      48(1).jpg   63.jpg     80(1).jpg   96(1).jpg
111(1).jpg  134.jpg     175.jpg    32(1).jpg   48(2).jpg   64(1).jpg  80(2).jpg   96(2).jpg
111(2).jpg  135.jpg     176.jpg    32(2).jpg   48.jpg      64(2).jpg  80.jpg      96.jpg
11(1).jpg   136.jpg     177.jpg    3(2).jpg    49(1).jpg   64.jpg     81(1).jpg   97(1).jpg
111.jpg     137.jpg     178.jpg    32.jpg      49(2).jpg   65(1).jpg  81(2).jpg   97(2).jpg
112(1).jpg  138.jpg     179.jpg    33(1).jpg   49.jpg      65(2).jpg  8(1).jpg    97.jpg
112(2).jpg  139.jpg     17.jpg     33(2).jpg   4.jpg       65.jpg     81.jpg      98(1).jpg
11(2).jpg   13.jpg      18(1).jpg   33.jpg      50(1).jpg   66(1).jpg  82(1).jpg   98(2).jpg
112.jpg     140.jpg     18(2).jpg   34(1).jpg   50(2).jpg   66(2).jpg  82(2).jpg   98.jpg
113(1).jpg  14(1).jpg   18.jpg     34(2).jpg   50.jpg      66.jpg     8(2).jpg    99(1).jpg
```

3) 提取照片的Exif信息

提取Exif信息使用的是Linux下面的**exiftool**,在Linux下可以使用如下命令安装：

Debian系的操作系统:

```
apt-get install exiftool
```

下面是批量提取**exif**信息的脚本

```
# pwd
/root/192.168.100.18
# for i in `ls`;do for j in `ls $i/*.jpg`;do echo "---$j---"; exiftool $j; done; d
one > ../exif-ftp.txt

# pwd
/root/Downloads/MISC3/all-jpg
# for i in `ls`; do echo "---$i---"; exiftool $i; done > exif-http.txt
```

运行完上面的命令后，会得到一个**exif-ftp.txt**和一个**exif-http.txt**

使用下面命令分别过滤出前半部分和后半部分flag：

```
 # grep '半' exif-http.txt
XP Comment                       : 恭喜你！找到一半了，还有另一半哦！flag{ae58d0408e26e8f
 # grep '半' exif-ftp.txt
XP Comment                       : 恭喜你！找到一半了，还有另一半哦！26a3c0589d23edeec}
```

拼接flag得到： flag{ **ae58d0408e26e8f26a3c0589d23edeec** }