31c3-ctf

misc

null。。

9477CTF

misc

coor coor

内存取证。。结合OTR聊天加密。
完全知识盲区。。
加上文件无法下载
只能pass

gecap

一个流量分析题
但是不是简单的流量分析或者是解密。
思路：流量包如果用现成的工具比如wireshark等去解析是永远无法得到有效消息的，需要手动去编辑解释器。通过010editor进行查看流量包，发现有一种块9447其中的内容没有能够被解析，将9447中的所有内容拼合起来是一个压缩包，解压以后得到flag。
（难点：知道wireshark分析的缺陷，且知道如何对流量包进行分析处理）

2014/asis-ctf-final

what-you-see

文件下载后是一个不知道什么东西的东西，原来是一种奇怪的压缩方式 ** xz compressed data **，

用unxz解压后得到 一个png图片。

> *unxz < milad_eb1ac478beffbbd33c564fbe6396042f > milad*

给出的png没有任何隐写信息，网上寻找原图，发现了一个大小不同的图片，（再找）。找到一个大小想同的图片，进行diff操作，得到下图

全黑？hahhh。
不是/
中间有变态红点。。然后把红点连起来是一只企鹅。
根据题目提示ASIS_MD5（）
所以flag就是ASIS_MD5(penguin)

tictac

一个奇怪文件，和上面一样是一个少有接触的压缩形式的压缩包。
解压得到一大串数字。

> *7069636b206d653a204153*
> *7069636b206d653a204153*
> *7069636b206d653a204953*
> *7069636b206d653a204953*
> *7069636b206d653a205f36*
> *7069636b206d653a206435*
> *7069636b206d653a206435*
> *7069636b206d653a203461*
> *7069636b206d653a203461*
> *7069636b206d653a203637*
> *7069636b206d653a203637*
> *7069636b206d653a203635*
> *7069636b206d653a203635*
> *7069636b206d653a203965*

> *7069636b206d653a203965*
> *7069636b206d653a203435*
> *7069636b206d653a206564*
> *7069636b206d653a206265*
> *7069636b206d653a203633*
> *7069636b206d653a206262*
> *7069636b206d653a206639*
> *7069636b206d653a203039*
> *7069636b206d653a203039*
> *7069636b206d653a206536*
> *7069636b206d653a206231*
> *7069636b206d653a203833*
> *7069636b206d653a203833*
> *7069636b206d653a206120*
> *7069636b206d653a206120*
> *7069636b206d653a20*

> *7069636b206d653a20*

第一行用hex-decode显示字符：pick me: AS
发现玄机。全部转化之后可以得到flag：

> *ASIS_6d54a67659e45edbe63bbf909e6b183a*

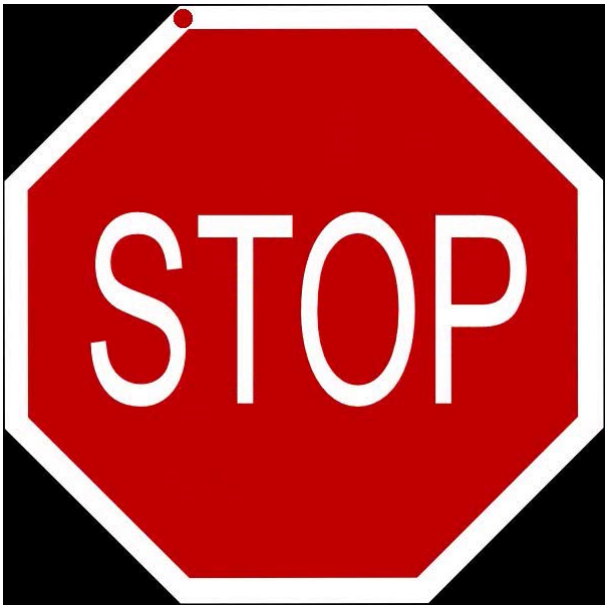
Stop!

一脉相承压缩，
解压可得文件。

一个视频文件，mpeg格式。
是对一个图标进行旋转的视频，肯定不会那么无聊啦，旋转后面铁定有信息。

> *STOP with no rotation and no dot: 0*

> *STOP with 135° rotation and no dot: 1*



将每一帧视频分离，可以用ffmpeg，convert等。进行手动转化信息，解码可得。

2014/asis-ctf-quals

censored array

需要nc。挂了。。
ACL Forensic

forensic-100

需要nc。

forensic-2

应该是一个系统盘取证题目，附件巨大。下载不稳定，一直失败。

forensic

得到一个流量包/
进行搜索分析，字符串查找flag。发现了一个相关的压缩包。
导出压缩包，进行解压发现又是一个pcap文件，再用wireshrke打开，结果发现打不开，损坏了。
需要对pcap进行一个修复操作。

> *pacpfix进行pcap修复操作*

里面一个压缩包，导出后可以查看到一个ASCII码处理的flag