DAY1

CTF-隐写

【题目附件】

附件下载

【实验任务】

```
从图片中找到flag值
```

解答思路：

首先查看该文件源码，查询到存在两个文件影写，观察结构后发现文件结构为jpg格式文件，新建文件后导出文件后ocr得到flag，bingo

```
flag{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}
```

CTF-流量分析

【题目附件】

附件下载

【实验任务】

```
从.pcap文件中获取flag值
```

解答思路：

直接wireshark打开后可以看见是较为常见的tcp与telnet，主要用作远程控制，直接追踪tcp数据流后，解出源码即可

```
flag{d316759c281bf925d600be698a4973d5}
```

CTF-密码学

【题目附件】

附件下载

【实验任务】

```
对密文进行解密得到flag值
```

解答思路：

简单古典密码，直接栅栏加凯撒直接解决

```
ssctf{_four#_sheep_}
```

CTF-磁盘取证

【题目附件】

附件下载

【实验任务】

```
在磁盘文件中获取到flag值
```

解答思路：

直接7zip打开知linux系统目录，尝试搜索后得知文件存在D:\Users\Downloads\file.zip\file\touch.dir\下，直接解答

```
flag{2h54k3d9i2b2o5d4r1s}
```

文本隐写

【题目附件】

附件下载

【实验任务】

```
word中的文本隐写
```

解答思路：

打开word后发现没有内容，用010打开后发现文件结构中存在flag字节，找到字节后找到对应文本块，直接复制粘贴即可

```
Flag{3e5twerfdtgg}
```

chrome plugin

【题目附件】

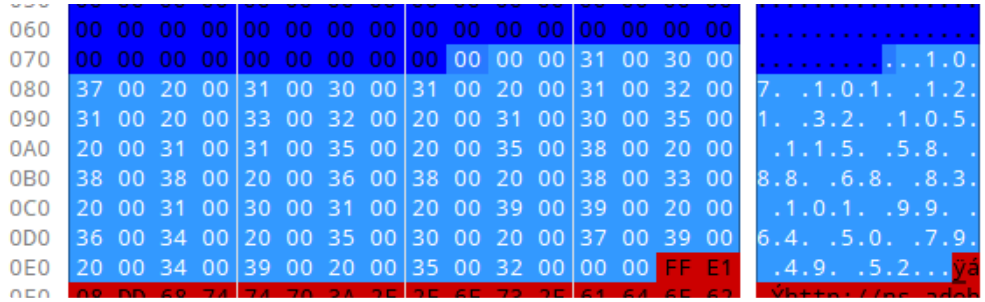
附件下载

【实验任务】

```
找到flag
```

解答思路：

7zip直接解压crx文件后得到插件具体目录，观察起文件结构后得知，js文件与html文件下均不存在flag，则对图片文件开始下手，观察其图片文件内存在



则使用解码工具解得答案，问题解出

```
flag{XDSec@2014}
```

男神一般都是很低调的

【题目附件】

附件下载

【实验任务】

```
找到隐藏的flag
```

解答思路：

简单的双图片影写，直接网上套工具解出

```
ctf{67a166801342415a6da8f0dbac591974}
```

音频隐写-频谱图隐写

【题目附件】

附件下载

【实验任务】

```
查看频谱图，发现隐写flag
```

解答思路：

观察文件，发现为单纯的音频文件，尝试播放后未发现内容，直接剪影查看波形图后解出答案

```
flag:e5353bb7b57578bd4da1c898a8e2d767
```

音频隐写-数据块隐写

【题目附件】

附件下载

【实验任务】

```
音频隐写-数据块隐写
```

解答思路：

解压后得到数据包，得知为一段音频加提示词，音频内容较为纯洁，暂时排除为混音音频，直接拖入010中解码可知，其文件无法查找具体的代码段，暂时放弃，后查看解析得知需用工具解决，下载工具MP3Stego后解出答案

```
SimCTF{MP3_MP3_sdfdsf}
```

【一招看懂压缩包分析】----【压缩包隐写出题介绍】实验1

【题目附件】

附件下载

【实验任务】

```
获取flag!
```

解答思路：

写的太快了，直接打开文件后，先点击txt查看文件内容后无果，再次点击照片后得到key.txt，观察内容可知4b05d3bc84fea85c255fa3dd63170865，大致为加密内容，解码后可知4b05d3bc84fea85c255fa3dd63170865

```
flag{www.simplexue.com}
```

【一招看懂压缩包分析】----【伪加密、爆破实战】实验1

【题目附件】

附件下载

【实验任务】

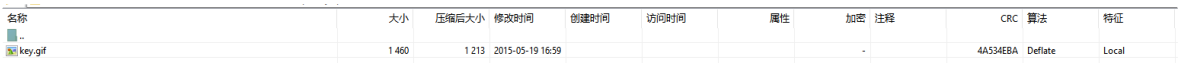
```
压缩包伪加密，找到flag!
```

解答思路：

7zip打开文件

名称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	加密	注释	CRC	算法	特征	主操作系统	版本	卷索引
..														
ekey.apk	1 361	1 366	2017-09-07 10:35	2018-06-21 14:15	2018-06-21 14:15	A	-		FC6BE128	Deflate	NTFS : UTF8	FAT	20	0

直接再次打开apk文件



名称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	加密	注释	CRC	算法	特征
..											
key.gif	1 460	1 213	2015-05-19 16:59				-		4A534EBA	Deflate	Local

解得key.gif文件

结束

```
KEY{4e8d5d998ab2de10}
```