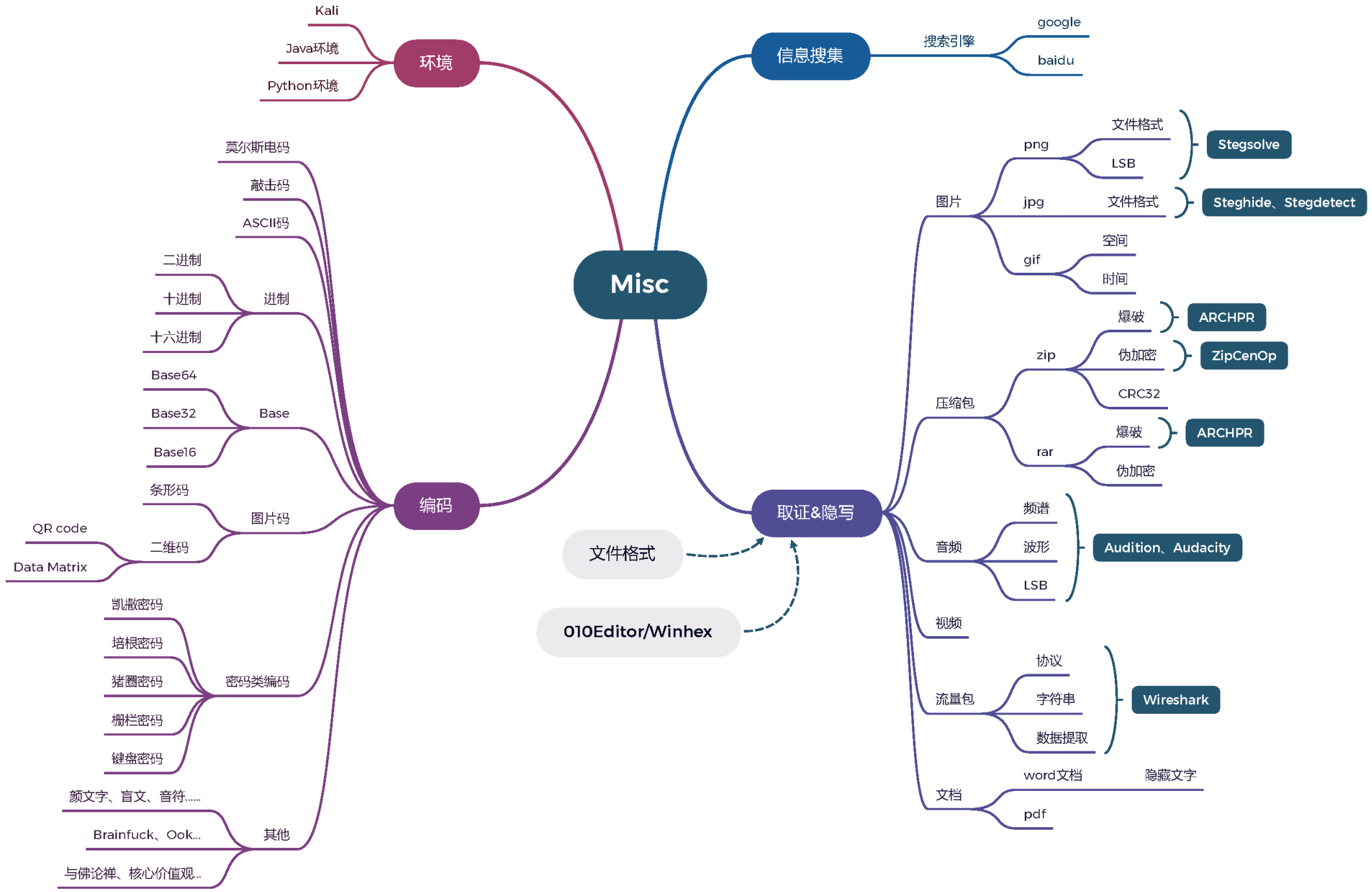
CTF-MISC概览

教师指导：游伟
学生指导：王浩潼

http://youwei.site/training/


Misc
环境
Kali
Java环境
Python环境
信息搜集
搜索引擎
google
baidu
编码
莫尔斯电码
敲击码
ASCII码
进制
二进制
十进制
十六进制
Base
Base64
Base32
Base16
图片码
条形码
二维码
QR code
Data Matrix
密码类编码
凯撒密码
培根密码
猪圈密码
栅栏密码
键盘密码
其他
颜文字、盲文、音符.....
Brainfuck、Ook...
与佛论禅、核心价值观...
取证&隐写
文件格式
010Editor/Winhex
图片
png
文件格式
LSB
Stegsolve
jpg
文件格式
Steghide、Stegdetect
gif
空间
时间
压缩包
zip
爆破
ARCHPR
伪加密
ZipCenOp
CRC32
rar
爆破
ARCHPR
伪加密
音频
频谱
波形
LSB
Audition、Audacity
视频
流量包
协议
字符串
数据提取
Wireshark
文档
word文档
隐藏文字
pdf

Misc

- 环境
- 信息搜集
- 编码
- 取证&隐写

环境

- Kali
- Java环境
- Python环境

信息搜集

- Google 基本搜索与挖掘技巧
- 保持简单明了的关键词
- 选择独特性的描述字词

- 地图和街景搜索
- 国外：Google Map、Google Earth、Google Street View
- 国内：百度地图、卫星地图、街景

信息搜集

- 例题：secret of bkfish

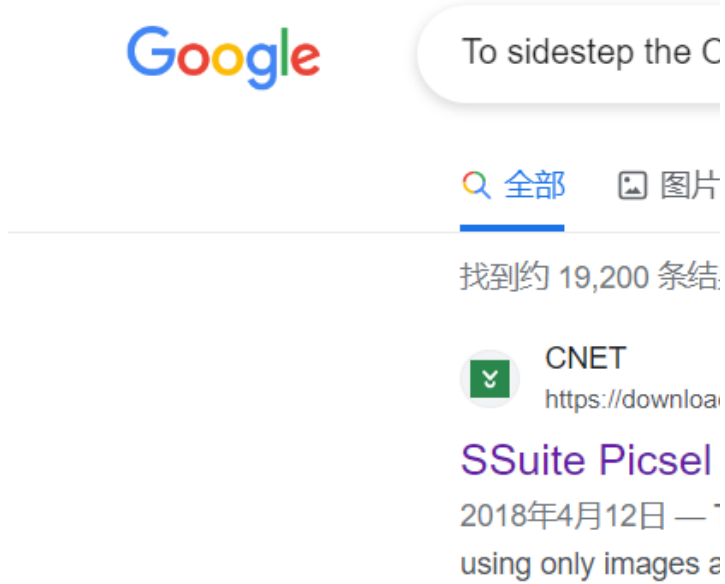
- To sidestep the Overlords of the internet ,bkfish use some real military grade encryption.

信息搜集

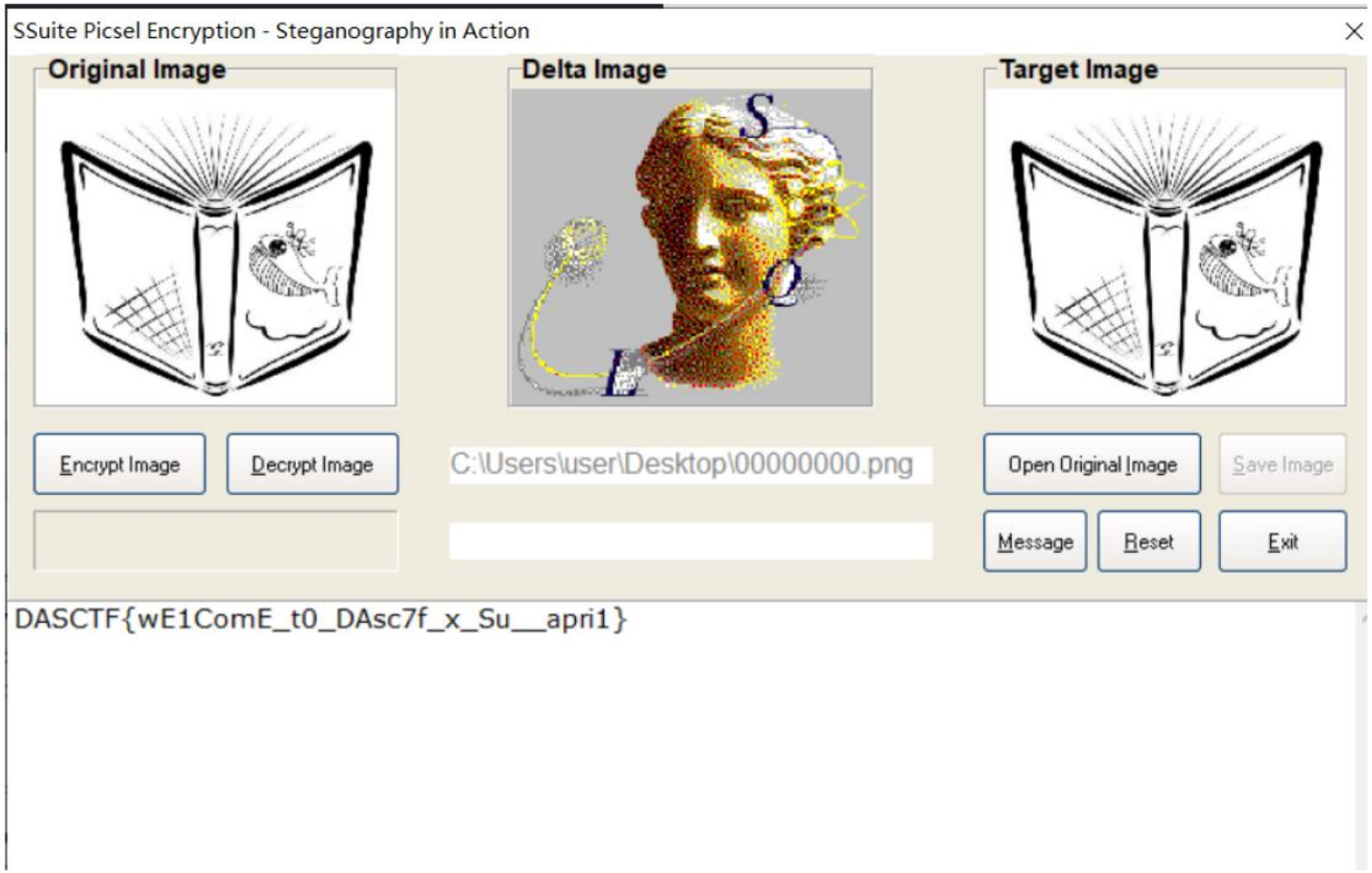
- 例题：secret of bkfish

信息搜集

- 例题：secret of bkfish



下载该工具对图片进行解密，小一点的图片作为Original img，大一点的图片作为decrypt img：



编码

- 莫尔斯编码
- 敲击码
- ASCII 编码
- 各种进制
- Base编码
- 图片码（条形码、二维码）
- 密码类编码
- 其他各种神奇编码

•编码-莫尔斯编码

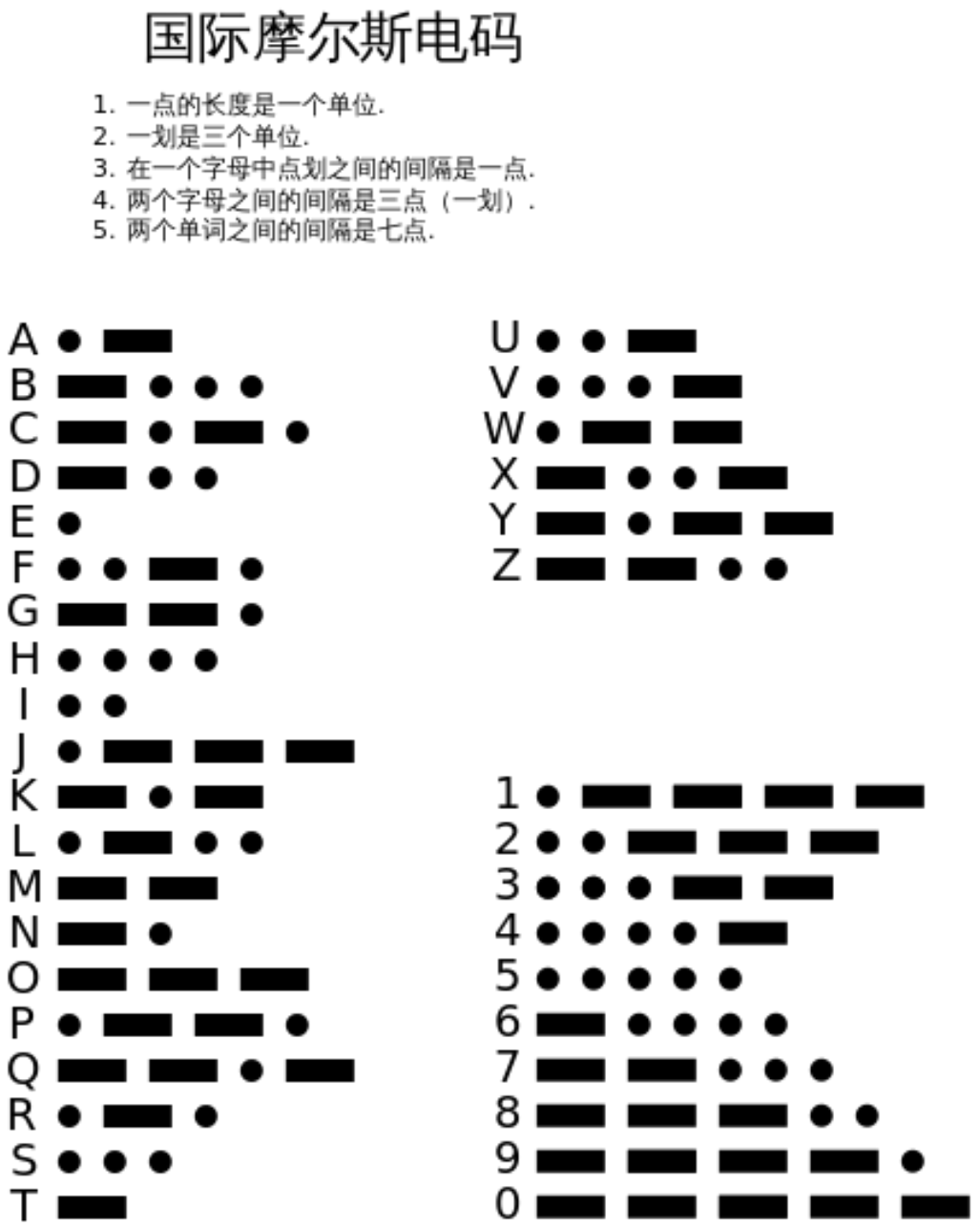
- 特点:

只有 . 和 -;

最多 6 位;

也可以使用 01 串表示。

- 摩尔斯编码在线转换:
  http://moersima.00cha.net/



•编码-敲击码

- 该编码对信息通过使用一系列的点击声音来编码而命名。

- 例：..... ../... ./... ./... .../
- 是敲击码，转换为 wllm

源文本	F	O	X
位置	2,1	3,4	5,3
敲击码	.. .	... .	....

Tap Code	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

编码-ASCII 编码

十进制	二进制	符号	十进制	二进制	符号	十进制	二进制	符号	十进制	二进制	符号
0	0000 0000	NUL	32	0010 0000	[空格]	64	0100 0000	@	96	0110 0000	`
1	0000 0001	SOH	33	0010 0001	!	65	0100 0001	A	97	0110 0001	a
2	0000 0010	STX	34	0010 0010	"	66	0100 0010	B	98	0110 0010	b
3	0000 0011	ETX	35	0010 0011	#	67	0100 0011	C	99	0110 0011	c
4	0000 0100	EOT	36	0010 0100	$	68	0100 0100	D	100	0110 0100	d
5	0000 0101	ENQ	37	0010 0101	%	69	0100 0101	E	101	0110 0101	e
6	0000 0110	ACK	38	0010 0110	&	70	0100 0110	F	102	0110 0110	f
7	0000 0111	BEL	39	0010 0111	'	71	0100 0111	G	103	0110 0111	g
8	0000 1000	BS	40	0010 1000	(	72	0100 1000	H	104	0110 1000	h
9	0000 1001	HT	41	0010 1001	)	73	0100 1001	I	105	0110 1001	i
10	0000 1010	LF	42	0010 1010	*	74	0100 1010	J	106	0110 1010	j
11	0000 1011	VT	43	0010 1011	+	75	0100 1011	K	107	0110 1011	k
12	0000 1100	FF	44	0010 1100	,	76	0100 1100	L	108	0110 1100	l
13	0000 1101	CR	45	0010 1101	-	77	0100 1101	M	109	0110 1101	m
14	0000 1110	SO	46	0010 1110	.	78	0100 1110	N	110	0110 1110	n
15	0000 1111	SI	47	0010 1111	/	79	0100 1111	O	111	0110 1111	o
16	0001 0000	DLE	48	0011 0000	0	80	0101 0000	P	112	0111 0000	p
17	0001 0001	DC1	49	0011 0001	1	81	0101 0001	Q	113	0111 0001	q
18	0001 0010	DC2	50	0011 0010	2	82	0101 0010	R	114	0111 0010	r
19	0001 0011	DC3	51	0011 0011	3	83	0101 0011	S	115	0111 0011	s
20	0001 0100	DC4	52	0011 0100	4	84	0101 0100	T	116	0111 0100	t
21	0001 0101	NAK	53	0011 0101	5	85	0101 0101	U	117	0111 0101	u
22	0001 0110	SYN	54	0011 0110	6	86	0101 0110	V	118	0111 0110	v
23	0001 0111	ETB	55	0011 0111	7	87	0101 0111	W	119	0111 0111	w
24	0001 1000	CAN	56	0011 1000	8	88	0101 1000	X	120	0111 1000	x
25	0001 1001	EM	57	0011 1001	9	89	0101 1001	Y	121	0111 1001	y
26	0001 1010	SUB	58	0011 1010	:	90	0101 1010	Z	122	0111 1010	z
27	0001 1011	ESC	59	0011 1011	;	91	0101 1011	[	123	0111 1011	{
28	0001 1100	FS	60	0011 1100	<	92	0101 1100	\	124	0111 1100	|
29	0001 1101	GS	61	0011 1101	=	93	0101 1101	]	125	0111 1101	}
30	0001 1110	RS	62	0011 1110	>	94	0101 1110	^	126	0111 1110	~
31	0001 1111	US	63	0011 1111	?	95	0101 1111	_	127	0111 1111	DEL

编码-各种进制

- 将 ascii 码对应的数字换成二进制、十六进制等表示形式。

•二进制:
•只有 0 和 1
•不大于 8 位，一般 7 位也可以，因为可见字符到 127。

•十六进制:
•A-Z→0x41~0x5A
•a-z→0x61~0x7A

编码-Base家族

- Base xx 中的 xx 表示的是采用多少个字符进行编码。
- 由于 2 的 6 次方等于 64，所以每 6 个比特为一个单元，对应某个可打印字符。3 个字节就有 24 个比特，对应于 4 个 Base64 单元，即 3 个字节需要用 4 个可打印字符来表示。

文本	M								a								n							
ASCII编码	77								97								110							
二进制位	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
索引	19				22				5				46											
Base64编码	T				W				F				u											

- B
- 特

ba

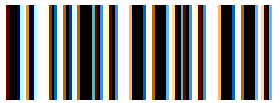
ba

根据 base 的不同，字符集会有所限制

Base全家桶工具：https://ctf.bugku.com/tools

编码-图片码

- 条形码



- 条形码在线识别：https://online-barcode-reader.inliteresearch.com/

- QR code二维码
- 工具：QR_Research、手机扫码、在线识别

- Datamatrix二维码
- DM码在线识别：https://jie.2weima.com/datamatrix.html

编码-密码类编码

- 凯撒密码、培根密码、猪圈密码、栅栏密码、键盘密码...

- 例:
- EWAZX RTY TGB IJN

- md5加密: https://www.sojson.com/encrypt_md5.html

编码-其他各种神奇编码

- 颜文字加密：http://www.atoolbox.net/Tool.php?Id=703
- 盲文加密：https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=mangwen
- 音乐符号加密：https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=yinyue
- Brainfuck/Ook：https://www.splitbrain.org/services/ook
- 与佛论禅加密：https://www.keyfc.net/bbs/tools/tudoucode.aspx
- 社会主义核心价值观加密：https://ctf.bugku.com/tool/cvecode
- Rot13：https://rot13.com/
- Twitter Secret Messages：https://holloway.nz/steg/

取证&隐写

- 前置技能
- 图片分析（PNG、JPG、GIF）
- 压缩包分析（ZIP、RAR）
- 音频&视频分析
- 流量包分析
- 文档分析

前置技能

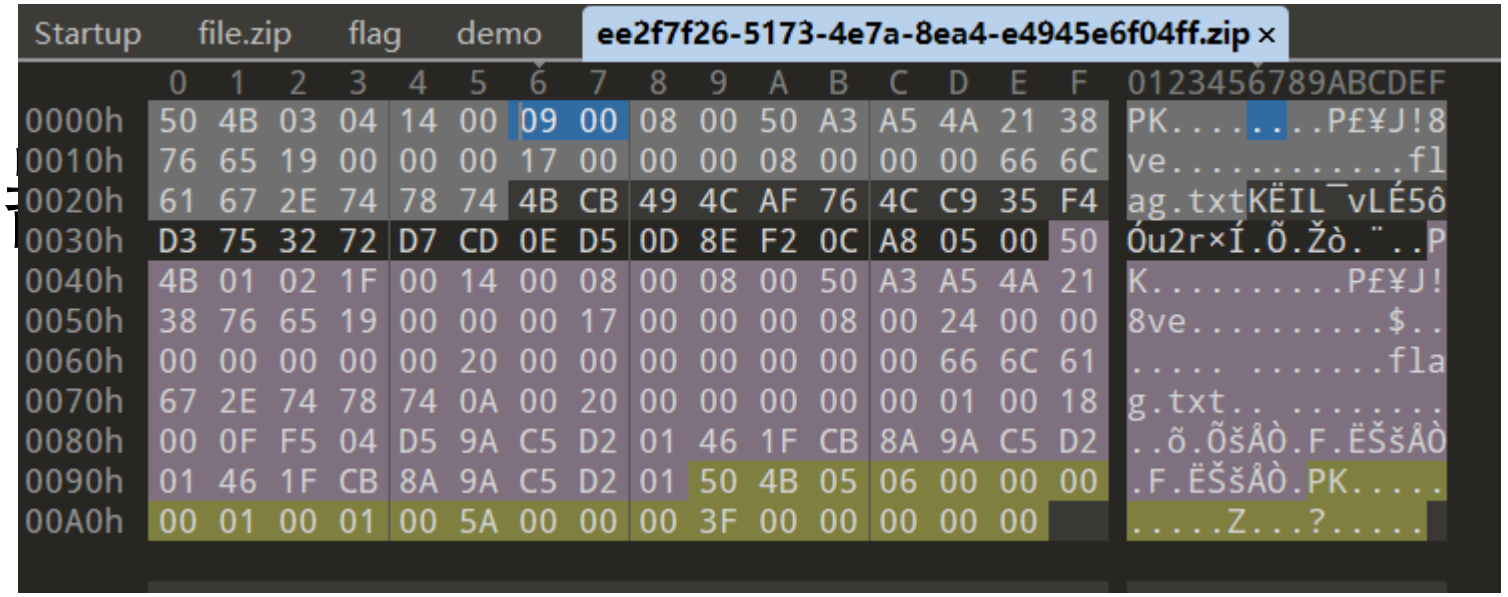
- 能够对文件中出现的一些编码进行解码，并且对一些特殊的编码（Base64、十六进制、二进制等）有一定的敏感度，对其进行转换并得到最终的 flag。
- 能够利用脚本语言（Python 等）去操作二进制数据
- 熟知常见文件的文件格式，尤其是各类 文件头、协议、结构等

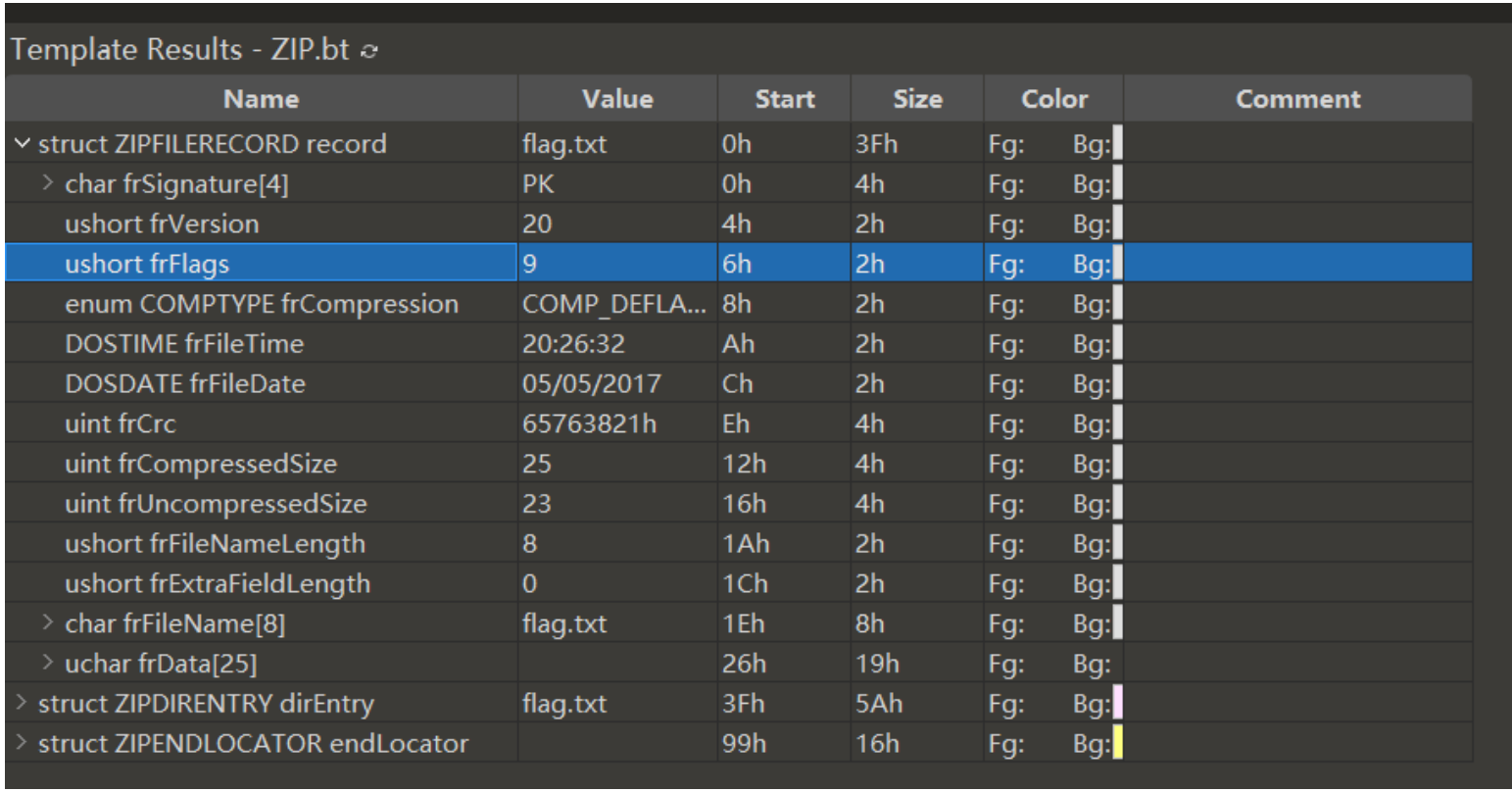
常见的文件头类型如图所示

文件类型	文件头
JPEG (jpg)	FFD8FFE1
PNG (png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053
Rich Text Format (rtf)	7B5C727466
XML (xml)	3C3F786D6C
HTML (html)	68746D6C3E
Adobe Acrobat (pdf)	255044462D312E
Wave (wav)	57415645
pcap (pcap)	4D3C2B1A

16进制文件编辑

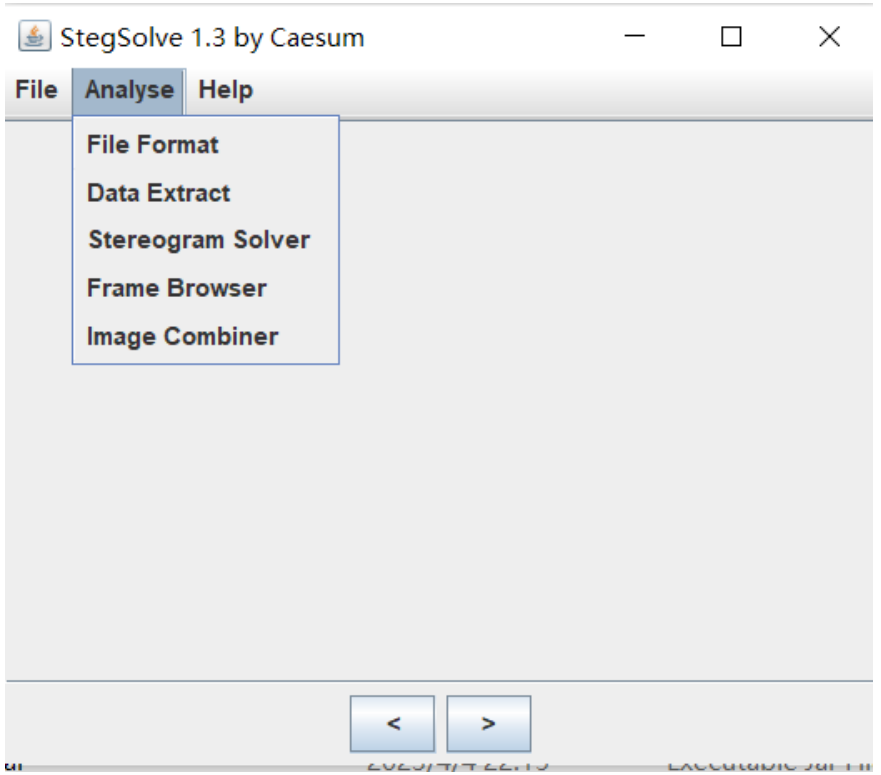
- 010Editor或Winhex





图片分析-PNG

- 文件格式IHDR：修改文件宽高隐藏信息
- LSB隐写：StegSolve提取LSB位
- 工具：StegSolve



图片分析-PNG

- 例题：　[BJDCTF2020]一叶障目
- LSB

图片分析-JPG

- 信息藏在图片数据中，用16进制文件编辑器找
- 有隐藏的文件，用binwalk或foremost分离
- 在属性信息中
- 注意JPG典型的文件头和文件尾，考虑合并、拆分文件
- 拼图

- 工具：Steghide
- Stegdetect：OutGuess、F5…

图片分析-JPG

- 例题：[ACTF新生赛2020]outguess
- outguess -k 'abc' -r mmm.jpg 1.txt
- 例题：[安洵杯 2019]吹着贝斯扫二维码

图片分析-GIF

- 逐帧分离:
- 可以用StegSolve的Frame Browser逐帧查看
- 可以将gif逐帧拆分静态图片（python脚本或其他工具）

- 时间轴：GIF 文件每一帧间的时间间隔也可以作为信息隐藏的载体。
- 通过identify命令清晰的打印出每一帧的时间间隔:
- `$ identify -format "%s %T \n" 100.gif`

图片分析-GIF

- 例题-逐帧分离:
- 金三胖

图片分析-GIF

- 例题-时间轴：
- XMAN-2017:100.gif

例如在当时在 XMan 选拔赛出的一题

> XMAN-2017:100.gif

通过 `identify` 命令清晰的打印出每一帧的时间间隔

```
$ identify -format "%s %T \n" 100.gif
0 66
1 66
2 20
3 10
4 20
5 10
6 10
7 20
8 20
9 20
10 20
11 10
12 20
13 20
14 10
15 10
```

推断 `20 & 10` 分别代表 `0 & 1`，提取每一帧间隔并进行转化。

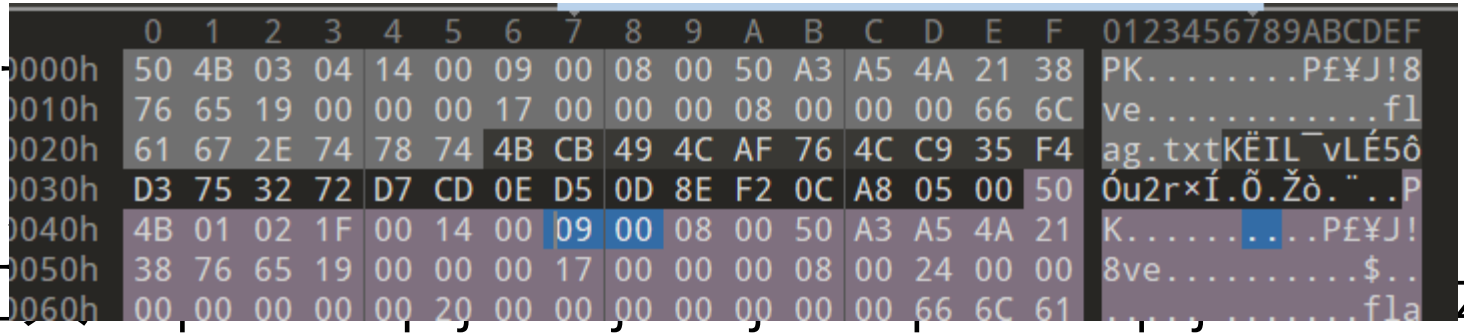
```
$ cat flag|cut -d ' ' -f 2|tr -d '66'|tr -d '\n'|tr -d '0'|tr '2' '0'
0101100001001101010000010100111001111011001110010011011000110101001101110011010101
```

最后转 ASCII 码得到 flag。

压缩包分析-ZIP

- 爆破：Windows神器ARCHPR，Linux命令行工具fcrackzip

- 伪加密：16进制
binwalk -e 无视伪
检测伪加密的小工 zip



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h	50	4B	03	04	14	00	09	00	08	00	50	A3	A5	4A	21	38	PK.....P£¥J!8
0010h	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C	ve.....fl
0020h	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4	ag.txtKËIL¯vLÉ5ô
0030h	D3	75	32	72	D7	CD	0E	D5	0D	8E	F2	0C	A8	05	00	50	Óu2r×Í.Õ.Žò.¨..P
0040h	4B	01	02	1F	00	14	00	09	00	08	00	50	A3	A5	4A	21	K.....P£¥J!
0050h	38	76	65	19	00	00	00	17	00	00	00	08	00	24	00	00	8ve.....$..
0060h	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	.....fla

- CRC32：
- 文件内内
- 加密的密
我们不去爆
都是可见的

Template Results - ZIP.bt

Name	Value	Start	Size	Color	Comment
struct ZIPDIRENTRY dirEntry	flag.txt	3Fh	5Ah	Fg: Bg:	
char deSignature[4]	PK	3Fh	4h	Fg: Bg:	
ushort deVersionMadeBy	31	43h	2h	Fg: Bg:	
ushort deVersionToExtract	20	45h	2h	Fg: Bg:	
ushort deFlags	9	47h	2h	Fg: Bg:	
enum COMPTYPE deCompression	COMP_DEFLA...	49h	2h	Fg: Bg:	
DOSTIME deFileTime	20:26:32	4Bh	2h	Fg: Bg:	
DOSDATE deFileDate	05/05/2017	4Dh	2h	Fg: Bg:	
uint deCrc	65763821h	4Fh	4h	Fg: Bg:	

压缩包分析-ZIP

- 例题：
- 爆破： ningen

- 伪加密： zip伪加密

- CRC32： zip

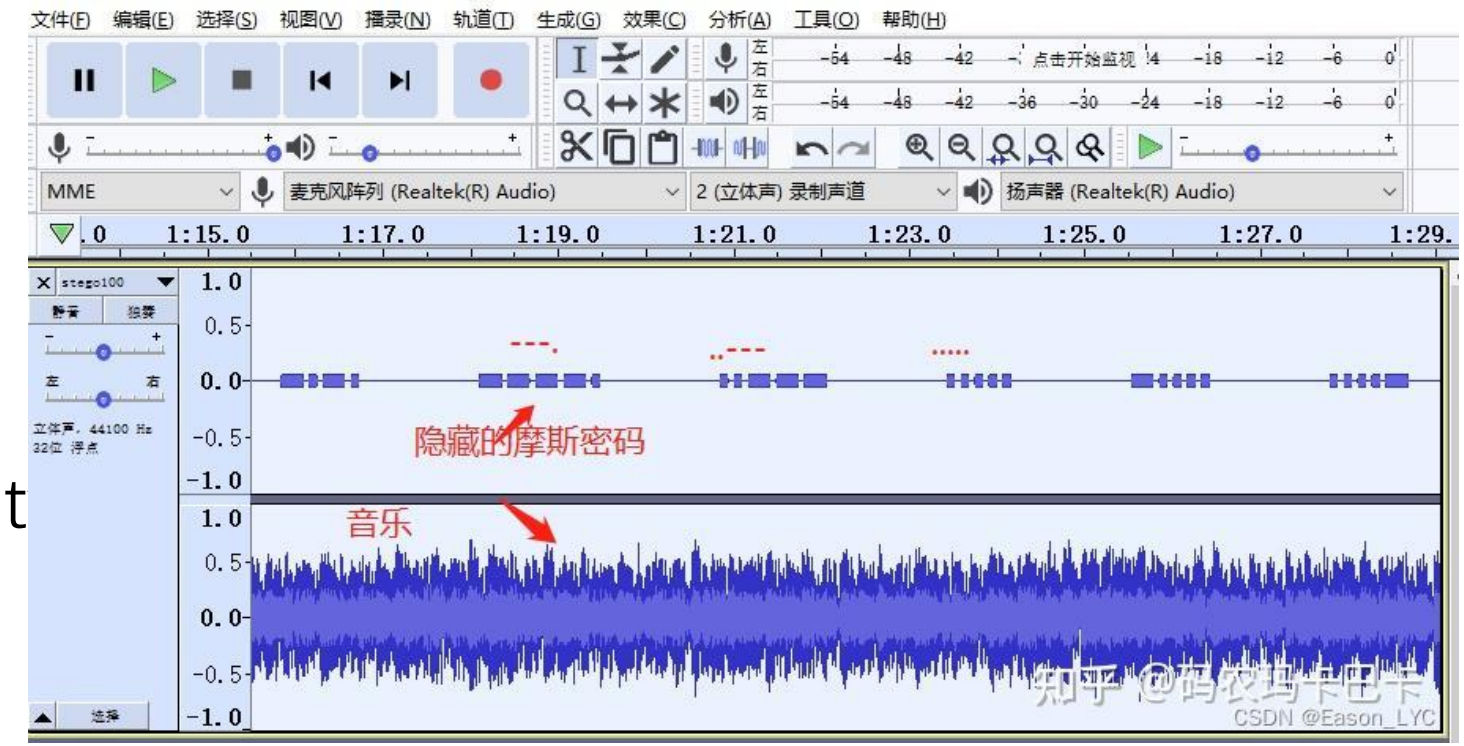
压缩包分析-RAR

- 爆破：Windows神器ARCHPR，Linux的RarCrack
- 伪加密：修改位

音频&视频分析

- 音频：摩斯电码
- 频谱、波形、LSB

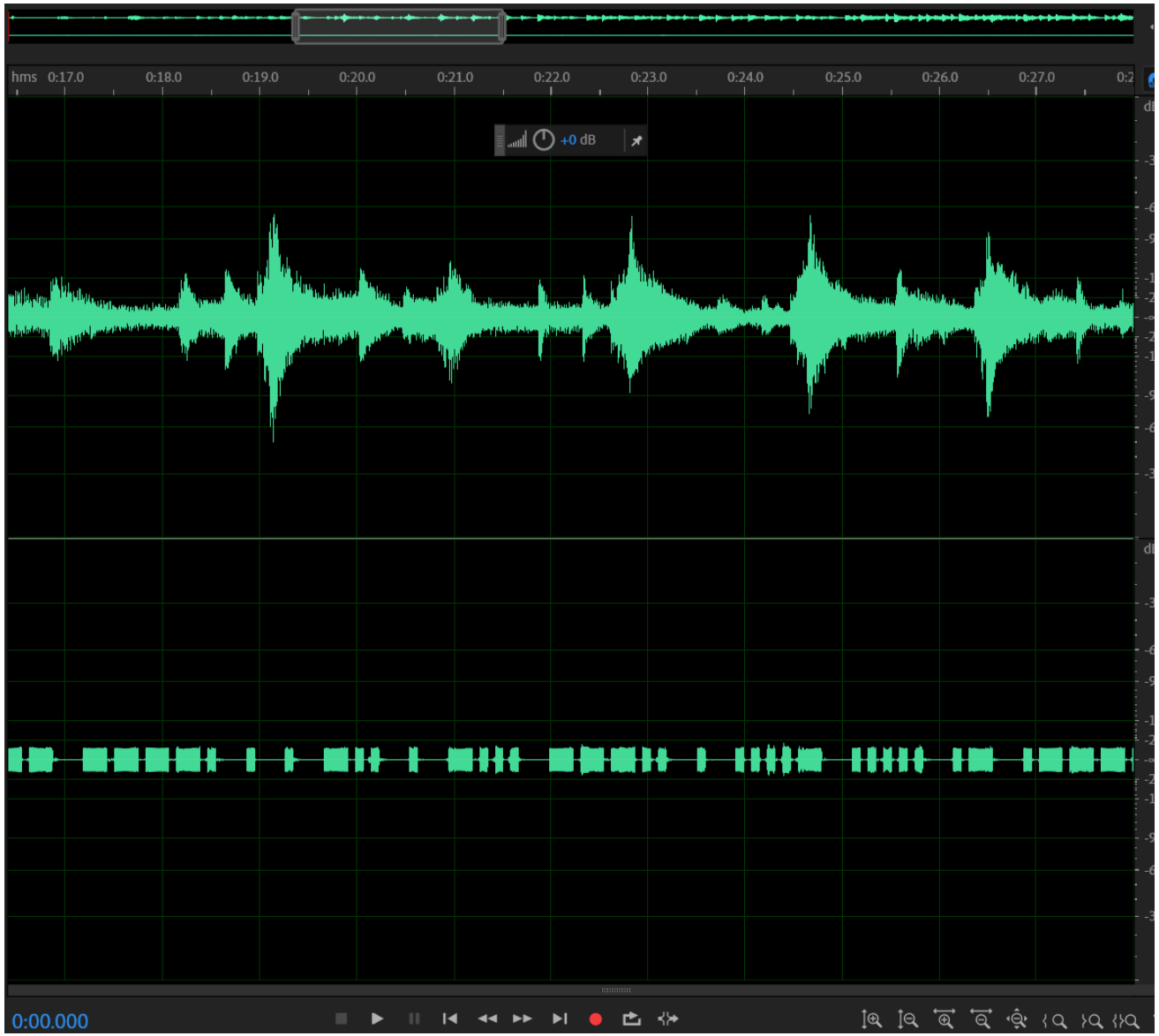
- 工具：Audition、Audacit



- 视频：视频中某帧有隐藏的信息
- 例题：[SWPU2019]你有没有好好看网课?

音频&视频分析

- 例题： 穿越时空的思念



流量包分析

- 工具：Wireshark

- 流量包修复
- pcapfix在线修复工具：http://f00l.de/hacking/pcapfix.php

- 协议：HTTP、TCP
- 解题思路：
- 1.用wireshark打开，分析http流和tcp流
- 2.搜索和flag有关的关键字（txt,flag,secret,zip），寻找信息,寻找进一步解题思路
- 3.导出http流和tcp流查看
- 4.如果传输中有可疑图片或者txt文件，可以分离出来进一步分析

- 数据提取
- 自动分析：file -> export objects -> http
- 手动分析：file->export selected Packet Bytes

流量包分析

- 例题：[CISCN2023]被加密的生产流量

- john-in-the-middle

文档分析

- word：隐藏文件(binwalk分离)、隐藏文字
- 例题：[MRCTF2020]你能看懂音符吗

- pdf：pdf中有图片，flag藏在图片下层
  （扩展）pdf隐写工具wbStego4open

综合题

- DASCTF Apr.2023 【简单】Ge9ian's Girl

- CISCN2023 国粹 （提示：buuoj 梅花香之苦寒来）

- 困难 CISCN2023 puzzle

分工学习

- 文件操作与隐写+压缩包处理（叶泽华）：

文件头；binwalk、foremost、dd文件分离；文件合并；压缩包破解、伪加密、攻击

- 图片、音频、视频隐写（梅祎航、杜海乐）：

Stegsolve使用；LSB隐写；PNG、JPG、GIF类常见隐写；其他隐写

- 流量取证技术（魏子洪、周小琳）：

Wireshark、tshark的使用；协议；常见流量（TCP、HTTP）；

进阶流量（蓝牙、USB、键盘鼠标）；特殊种类流量（工控、Modbus）

- 参考：CTF Wiki： https://ctf-wiki.org/misc/introduction/