20190815网络与信息安全领域专项赛线上赛misc WriteUp

转载

afu42832 于 2019-08-17 00:42:00 发布 162 收藏
文章标签： java 密码学 运维
原文链接：http://www.cnblogs.com/hardcoreYutian/p/11367003.html

目录

几星期前报了名却完全忘记了比赛，队长下发题目的时候我还以为是他偷偷报名参加的比赛，发题目让我们练习练习呢。。（在我多次逼问后才得到事情的真相）于是在比赛结束后开始做，完成了3道misc的解答，膜拜队长ak了4道。

签到题

此题是在队长的指点下完成的，佩服队长的博学。

题目内容

使用工具

nslookup

解题步骤

知道的便是知道，不知道的经历这次后应当知道。这题需要了解 dns 的 txt记录，我们查看的方式是在命令行使用 nslookup 工具。

直接得到flag。

七代目

题目下载地址

https://pan.baidu.com/s/1UuKHAyGThElHdxZlVygUSw 解压密码：tzzo

使用工具

winhex，Stegsolve.jar下载地址

解题步骤

1.下载下来是一个压缩包，解压后是一个 .gif 文件，但是损坏了打不开。

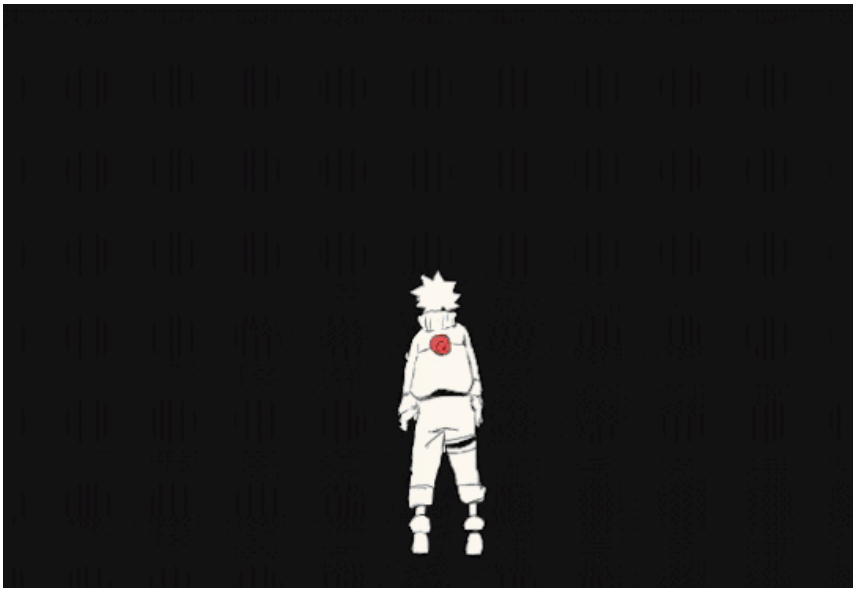
七代目.gif
无法打开此文件。

无是使用winhex打开，发现文件头错误，改成 .gif 的文件头 47494638，修复成功

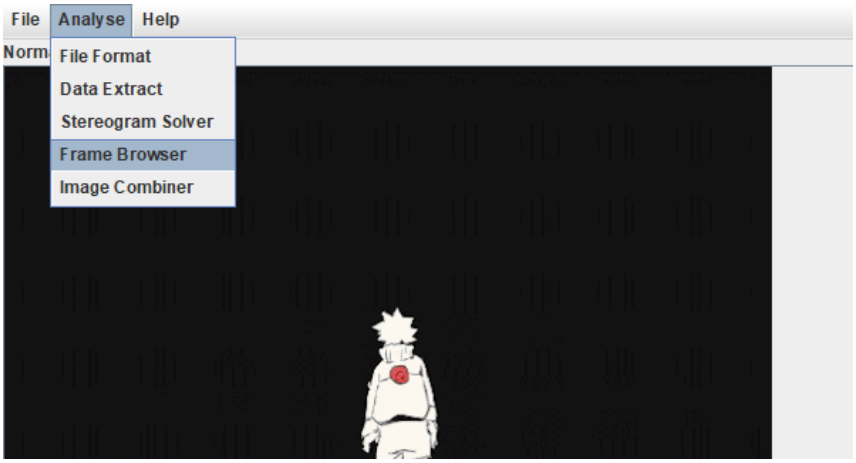
了是使用winhex打开，发现文件头错误，改成 .gif 的文件头 47494638，修复成功。

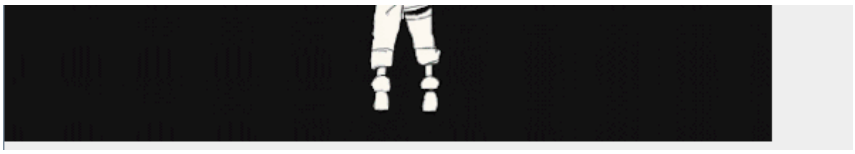
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	89	50	4E	47	39	61	1C	02	73	01	F6	09	00	12	12	12	塒NG9a..s.?....
00000010	10	08	10	08	08	10	27	25	24	64	5A	5C	07	07	07	C6	......'%$dZ\...?
00000020	C6	C6	42	42	42	BC	BC	BC	FC	F8	F0	73	73	73	8C	8C	破BBB技键 sss寤
00000030	8C	78	8E	84	EB	EB	E9	5A	59	59	DA	D6	DA	A7	A7	A5	青鸯脭閆YY谧讧卩
00000040	55	52	4A	F9	EE	E8	99	98	96	11	10	08	FA	F7	ED	39	URJ 铡槱... ?
00000050	39	39	EF	F7	EF	D8	CE	C8	EA	E7	DC	08	11	10	CD	D6	99秣镓稳赙?..椭
00000060	CB	EC	E3	E0	C1	BD	C6	AD	97	8A	B5	5A	61	8D	6B	4E	遂泛两骗棲礪a.kN
00000070	98	2A	1D	6E	38	27	F2	D7	D2	60	44	34	DD	3E	42	D5	?.n8'蜃禊D4?B?
00000080	59	64	F4	52	4D	CD	33	27	FF	E7	F1	F3	B8	B1	DE	94	Yd髯M?' 珩蟾鞭?
00000090	6C	D7	98	95	F4	58	63	5A	5A	63	06	06	06	05	05	05	l譴瞩XcZZc.....
000000A0	04	04	04	EC	E8	E0	B9	B6	B0	A2	A2	A0	A2	9F	A2	B7	...扈喙栋ii牖煝?
000000B0	BF	B5	01	01	01	00	00	00	03	03	03	02	02	02	53	53	康.....SS
000000C0	52	02	03	03	12	11	0F	0B	0B	0B	6B	6B	6A	3E	3E	3E	R.....kkj>>>
000000D0	10	10	10	17	17	17	29	29	29	20	1E	1D	12	10	10	11	.....))) .....
000000E0	11	11	14	14	14	83	81	7D	7E	7C	78	81	81	81	D3	B2	.....?}~|x...硬
000000F0	A3	75	19	21	F7	6A	50	A7	86	63	FE	F7	DC	F7	D0	B2	.!鰳P c 荀胁
00000100	FA	9F	A1	E6	78	81	FE	ED	D9	FD	DB	CA	F2	F1	CE	F4	赢℃x. 洌幽螳昔

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	47	49	46	38	39	61	1C	02	73	01	F6	09	00	12	12	12	GIF89a..s.?....
00000010	10	08	10	08	08	10	27	25	24	64	5A	5C	07	07	07	C6	......'%$dZ\...?
00000020	C6	C6	42	42	42	BC	BC	BC	FC	F8	F0	73	73	73	8C	8C	破BBB技键 sss寤
00000030	8C	78	8E	84	EB	EB	E9	5A	59	59	DA	D6	DA	A7	A7	A5	青鸯脭閆YY谧讧卩
00000040	55	52	4A	F9	EE	E8	99	98	96	11	10	08	FA	F7	ED	39	URJ 铡槱... ?
00000050	39	39	EF	F7	EF	D8	CE	C8	EA	E7	DC	08	11	10	CD	D6	99秣镓稳赙?..椭
00000060	CB	EC	E3	E0	C1	BD	C6	AD	97	8A	B5	5A	61	8D	6B	4E	遂泛两骗棲礪a.kN
00000070	98	2A	1D	6E	38	27	F2	D7	D2	60	44	34	DD	3E	42	D5	?.n8'蜃禊D4?B?
00000080	59	64	F4	52	4D	CD	33	27	FF	E7	F1	F3	B8	B1	DE	94	Yd髯M?' 珩蟾鞭?
00000090	6C	D7	98	95	F4	58	63	5A	5A	63	06	06	06	05	05	05	l譴瞩XcZZc.....
000000A0	04	04	04	EC	E8	E0	B9	B6	B0	A2	A2	A0	A2	9F	A2	B7	...扈喙栋ii牖煝?
000000B0	BF	B5	01	01	01	00	00	00	03	03	03	02	02	02	53	53	康.....SS
000000C0	52	02	03	03	12	11	0F	0B	0B	0B	6B	6B	6A	3E	3E	3E	R.....kkj>>>
000000D0	10	10	10	17	17	17	29	29	29	20	1E	1D	12	10	10	11	.....))) .....
000000E0	11	11	14	14	14	83	81	7D	7E	7C	78	81	81	81	D3	B2	.....?}~|x...硬
000000F0	A3	75	19	21	F7	6A	50	A7	86	63	FE	F7	DC	F7	D0	B2	.!鰳P c 荀胁

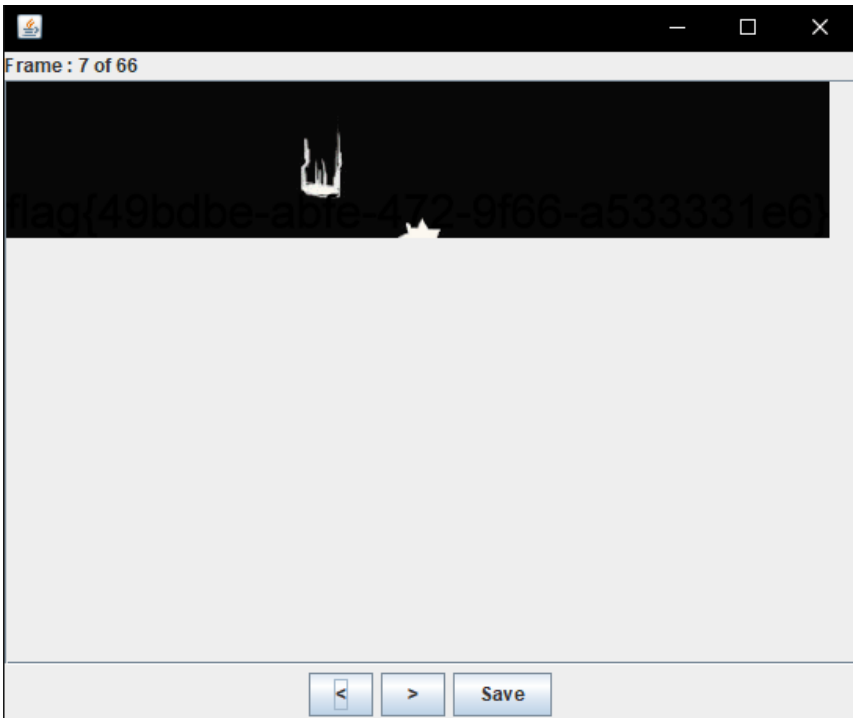


2.然后对于这张gif图片，我使了一大堆招都木用。在电脑上配置好Java环境，下载Stegsolve.jar，然后到命令行中移动到下载的目录使用`java -jar stegsolve.jar`可以使用Stegsolve工具。使用此工具可以对gif图片逐帧分离。这张图片逐帧分离共有66张，一张张地处理分析工作量太大不可取。

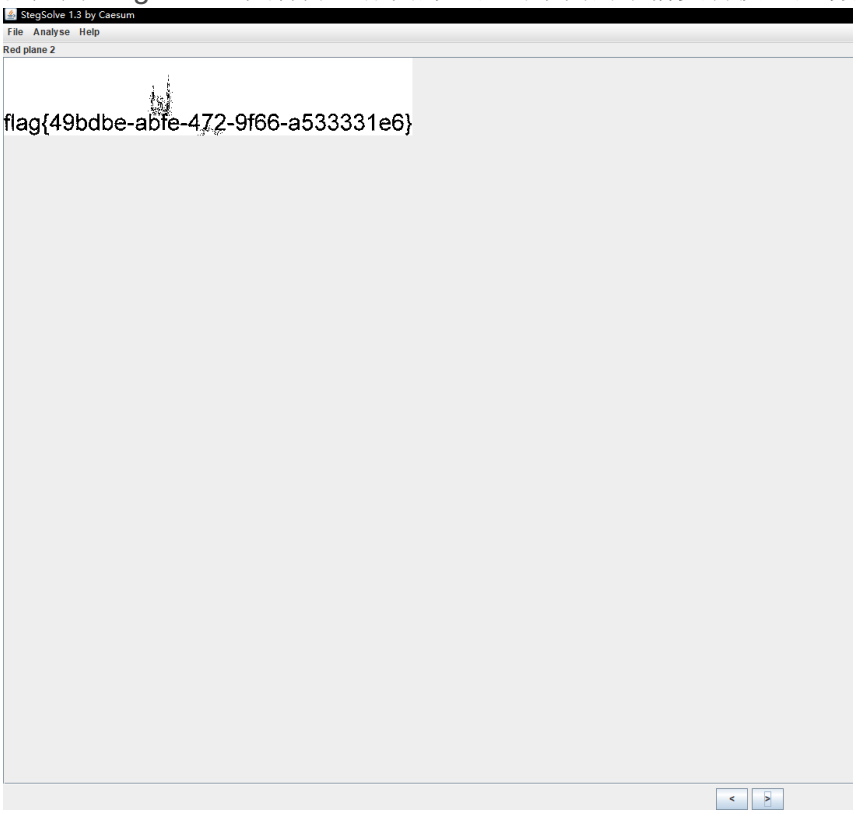




我想，为啥这题叫“七代目”呢？我尝试在写着“七代目”的披风上做文章，并没有什么用。再想想，七代目，七，7，第7张！于是保存逐帧分离的第7张图片



然后用Stegsolve工具打开这张图片，点击下面的小箭头切换，点着点着就得到flag啦~



亚萨西

题目下载链接

https://pan.baidu.com/s/1wD36mEzc0eY_GSsNHcA9Wg 解压码：0try

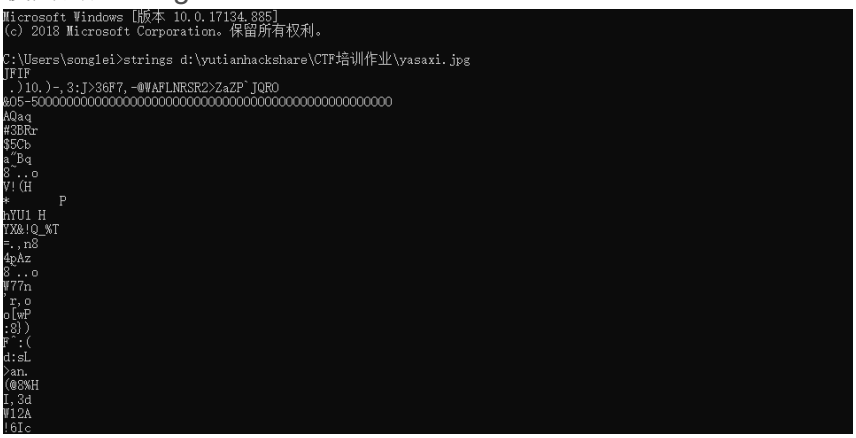
使用工具

Ziperello，strings，Ook!在线解密网站

解题步骤

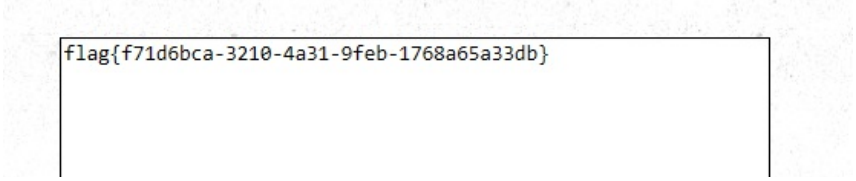
1.下载下来是一个压缩包，尝试解压发现有解压密码，于是使用 Ziperello 进行字典爆破。密码是 loli 눈_눈。

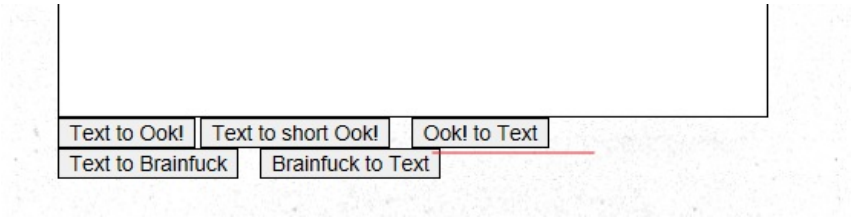
2.解压完里面是一张图片，接下来你可以使用 winhex，strings，010editor 等等任意工具，查看它的字符串。我使用的是strings



往下拖呀拖，会发现末尾的一堆符号特别可疑！全是 .!? 这三个符号组成的，盲猜是一种加密方式。

于是去网上找CTF密码学入门的帖子，逐渐找到一个叫 Ook! 的东西，它的特点就是内容全为 Ook和 .!? 这三个字符。然后我一开始想把这个图片下面的这些符号前依次加上 Ook ，并去掉所以空格，不过实在太多太麻烦了，于是我尝试不加修改，直接在在线的解密网站里粘贴这段符号，发现可以直接解出flag。





24word

题目下载链接

https://pan.baidu.com/s/13_6CqQUnHyDAPKvuJnOlMQ 解压码:bsmh

使用工具

社会主义核心价值观在线解密工具，binwalk，dd

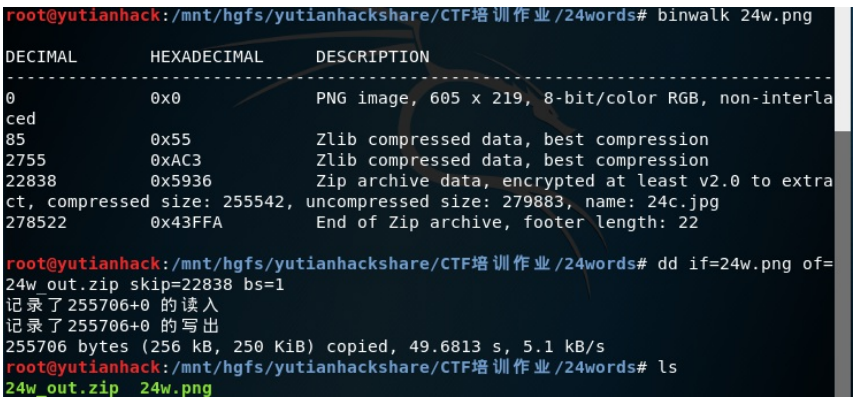
解题步骤

1.下载下来是个压缩包，解压之，里面是一张人畜无害的图片 24w.png

无需怀疑，这明显是核心价值观加密，于是我们使用在线网站进行解密，输入图片中的文字内容

得到一个结果 CodeValues，百度搜索一下会发现可口可乐的网站（雾）。

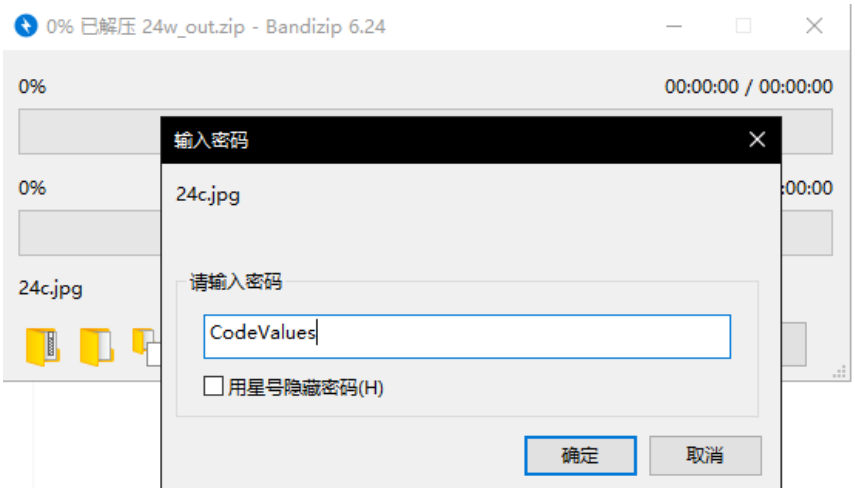
2.仔细看看，这张浓眉大眼的图片 24w.png 其实并不简单！何以言之？使用binwalk，发现图片里暗藏压缩包，于是使用 dd 分离出来



由 binwalk 可知 zip文件开始处为22838，所以 dd 的指令是`dd if=24w.png of=24w_out.zip`

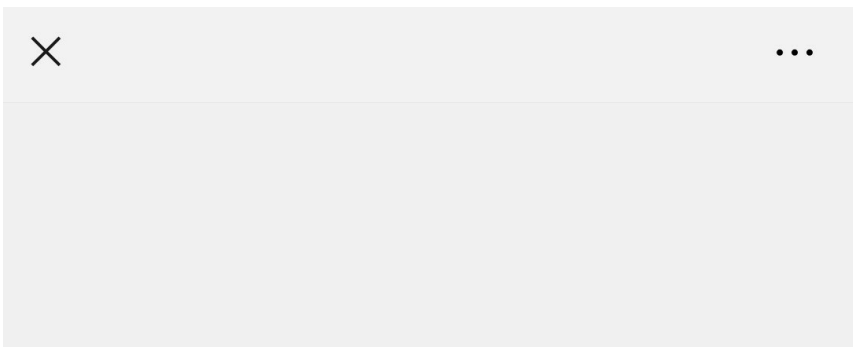
skip=22838 bs=1，分离出一个文件命名为 24w_out.zip 。

3.尝试解压这个 24w_out.zip文件，发现需要解压密码，这时我们使用第一步得到的 CodeValues 完成解压。



4.解压出来又是一张图片 24c.jpg ， 内容是完整的核心价值观。

定睛多看几遍，图片下面是一张斜着的二维码呀！直接拿手机扫描一下得到flag。



未找到 flag{24_word_m4n7ra} 的相关信息

感想

感觉要犯脊椎病了。

转载于:https://www.cnblogs.com/hardcoreYutian/p/11367003.html