Misc : Layouts

Description : Sherlock found a huge pile of evidence, but it was difficult for him to analyze them. Help him.

Attachment : RWtm7A5f

Solution :

First download the attachment «Rwtm7A5f». Using «file» against the file show us its a zip archive.

```
root@kali:~/Téléchargements/layouts# file RWtm7A5f
RWtm7A5f: Zip archive data, at least v2.0 to extract
```

Trying to extract it but it ask for password, trying the name of the zip as password worked, but it seem to be a loop, cause there is another zip protected with the file name as password again and again. So i make a little bash script for automate the process.

```
#!bin/sh

zipfile="RWtm7A5f" #Give the value of the first zip to extract as zipfile variable.

#Make a while who unzip the archive "zipfile" with the zip file name as password
while unzip -P "$zipfile" "$zipfile"; do
        next_zipfile="$(unzip -Z1 "$zipfile" | head -n1)" #Take the next zip file name
        zipfile="$next_zipfile" #Overwrite the zipfile variable and put the next zip file instead
done
```

Give the script execution right with «chmod +x» then run it. At the end it will extract an archive named «flag».

```
Archive:  kSPrXQjZ
 extracting: flag
Archive:  flag
  End-of-central-directory signature not found.  Either this file is not
  a zipfile, or it constitutes one disk of a multi-part archive.  In the
  latter case the central directory and zipfile comment will be found on
  the last disk(s) of this archive.
unzip:  cannot find zipfile directory in one of flag or
        flag.zip, and cannot find flag.ZIP, period.
root@kali:~/Téléchargements/layouts#
```

Extract the «flag» archive, and we get a directory with many sub-directory.

```
root@kali:~/Téléchargements/layouts/flag (1)/flags# ls
1    112  126  14   153  167  180  194  207  220  234  248  31  45  59  72  86
10   113  127  140  154  168  181  195  208  221  235  249  32  46  6   73  87
100  114  128  141  155  169  182  196  209  222  236  25   33  47  60  74  88
101  115  129  142  156  17   183  197  21   223  237  250  34  48  61  75  89
102  116  13   143  157  170  184  198  210  224  238  251  35  49  62  76  9
103  117  130  144  158  171  185  199  211  225  239  252  36  5   63  77  90
104  118  131  145  159  172  186  2    212  226  24   253  37  50  64  78  91
105  119  132  146  16   173  187  20   213  227  240  254  38  51  65  79  92
106  12   133  147  160  174  188  200  214  228  241  255  39  52  66  8   93
107  120  134  148  161  175  189  201  215  229  242  26   4   53  67  80  94
108  121  135  149  162  176  19   202  216  23   243  27   40  54  68  81  95
109  122  136  15   163  177  190  203  217  230  244  28   41  55  69  82  96
11   123  137  150  164  178  191  204  218  231  245  29   42  56  7   83  97
110  124  138  151  165  179  192  205  219  232  246  3    43  57  70  84  98
111  125  139  152  166  18   193  206  22   233  247  30   44  58  71  85  99
```

I used tree for see exactly which content have this «flag» directory.

```
root@kali:~/Téléchargements/layouts/flag (1)/flags# tree
.
├── 1
├── 10
├── 100
├── 101
│   └── 9
├── 102
│   └── 11
├── 103
│   └── 8
├── 104
├── 105
├── 106
├── 107
├── 108
├── 109
├── 11
├── 110
│   └── 16
├── 111
├── 112
│   └── 18
├── 113
```

As we can note, we get many directory, the directory have number as name, inside few directory, we have some empty files, there name is number too, but we can note the file are the number 1 to 21.

So taking the directory name as file order and we get a string of numbers.

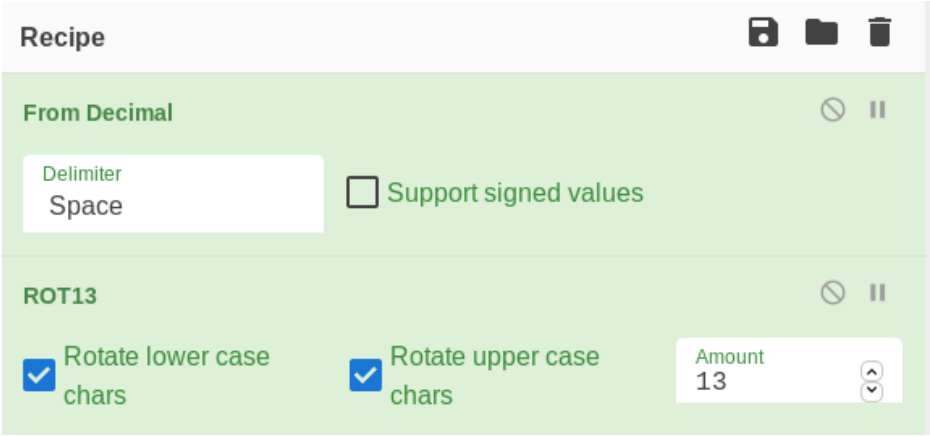
For exemple, if file «1» is inside the folder «58» and file «2» is inside the folder «120» our string will start by «58 120 ...».

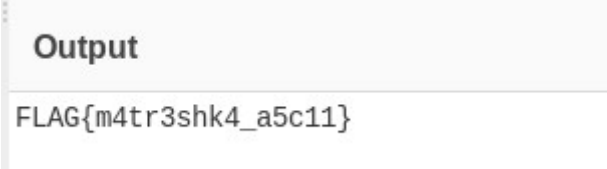
Complete string in order :

83 89 78 84 123 122 52 103 101 51 102 117 120 52 95 110 53 112 49 49 125

Searching a while on google for decode that strings and i found the cipher was a combination of «From decimal and Rot 13», i used cyber chef for do that.

Source :
https://gchq.github.io/CyberChef/#recipe=From_Decimal('Space',false)ROT13(true,true,13)





Flag : FLAG{m4tr3shk4_a5c11}