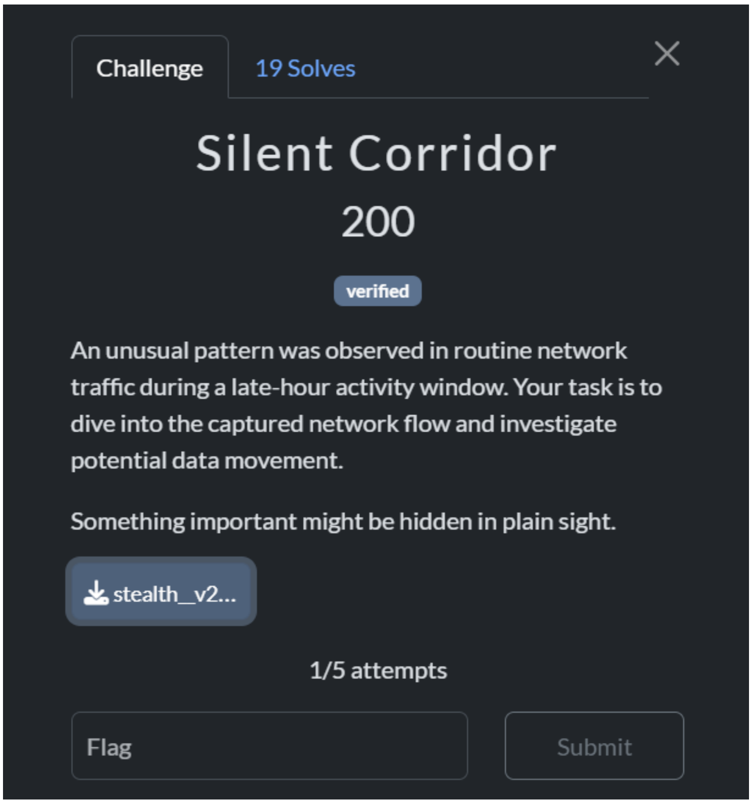
Challenge Name: Silent Corridor — 200pts (Forensics)



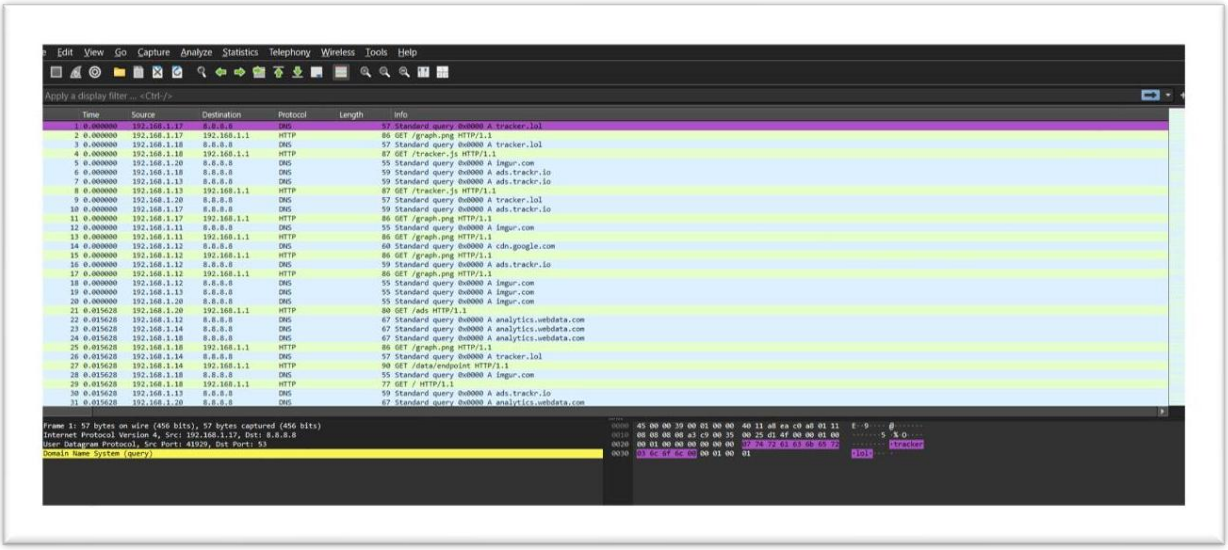
Silent Corridor

200

An unusual pattern was observed in routine network traffic during a late-hour activity window. Your task is to dive into the captured network flow and investigate potential data movement.

Something important might be hidden in plain sight.

Here I got the pcap file, I downloaded that and start investigating it.



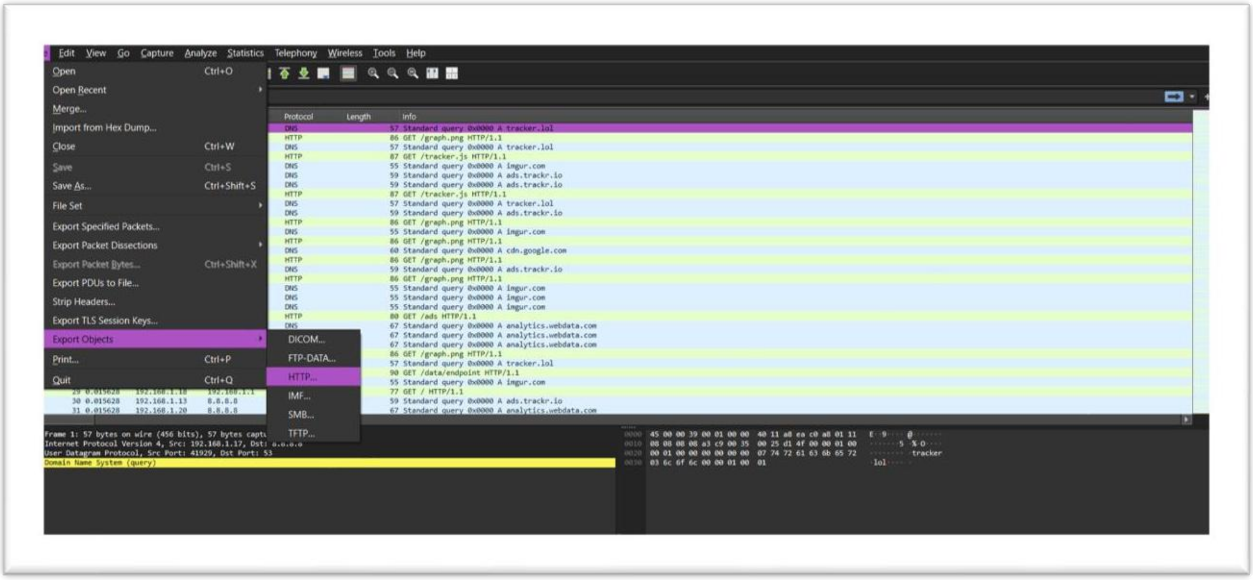
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
    Time      Source        Destination   Protocol  Length  Info
  1 0.000000  192.168.1.17  8.8.8.8       DNS               57 Standard query 0x0000 A tracker.lol
  2 0.000000  192.168.1.17  192.168.1.1   HTTP              86 GET /graph.png HTTP/1.1
  3 0.000000  192.168.1.18  8.8.8.8       DNS               57 Standard query 0x0000 A tracker.lol
  4 0.000000  192.168.1.18  192.168.1.1   HTTP              87 GET /tracker.js HTTP/1.1
  5 0.000000  192.168.1.20  8.8.8.8       DNS               55 Standard query 0x0000 A imgur.com
  6 0.000000  192.168.1.18  8.8.8.8       DNS               59 Standard query 0x0000 A ads.trackr.io
  7 0.000000  192.168.1.13  8.8.8.8       DNS               59 Standard query 0x0000 A ads.trackr.io
  8 0.000000  192.168.1.13  192.168.1.1   HTTP              87 GET /tracker.js HTTP/1.1
  9 0.000000  192.168.1.20  8.8.8.8       DNS               57 Standard query 0x0000 A tracker.lol
 10 0.000000  192.168.1.17  8.8.8.8       DNS               59 Standard query 0x0000 A ads.trackr.io
 11 0.000000  192.168.1.17  192.168.1.1   HTTP              86 GET /graph.png HTTP/1.1
 12 0.000000  192.168.1.11  8.8.8.8       DNS               55 Standard query 0x0000 A imgur.com
 13 0.000000  192.168.1.11  192.168.1.1   HTTP              86 GET /graph.png HTTP/1.1
 14 0.000000  192.168.1.12  8.8.8.8       DNS               60 Standard query 0x0000 A cdn.google.com
 15 0.000000  192.168.1.12  192.168.1.1   HTTP              86 GET /graph.png HTTP/1.1
 16 0.000000  192.168.1.12  8.8.8.8       DNS               59 Standard query 0x0000 A ads.trackr.io
 17 0.000000  192.168.1.12  192.168.1.1   HTTP              86 GET /graph.png HTTP/1.1
 18 0.000000  192.168.1.12  8.8.8.8       DNS               55 Standard query 0x0000 A imgur.com
 19 0.000000  192.168.1.13  8.8.8.8       DNS               55 Standard query 0x0000 A imgur.com
 20 0.000000  192.168.1.20  8.8.8.8       DNS               55 Standard query 0x0000 A imgur.com
 21 0.015628  192.168.1.20  192.168.1.1   HTTP              80 GET /ads HTTP/1.1
 22 0.015628  192.168.1.12  8.8.8.8       DNS               67 Standard query 0x0000 A analytics.webdata.com
 23 0.015628  192.168.1.14  8.8.8.8       DNS               67 Standard query 0x0000 A analytics.webdata.com
 24 0.015628  192.168.1.18  8.8.8.8       DNS               67 Standard query 0x0000 A analytics.webdata.com
 25 0.015628  192.168.1.18  192.168.1.1   HTTP              86 GET /graph.png HTTP/1.1
 26 0.015628  192.168.1.14  8.8.8.8       DNS               57 Standard query 0x0000 A tracker.lol
 27 0.015628  192.168.1.14  192.168.1.1   HTTP              90 GET /data/endpoint HTTP/1.1
 28 0.015628  192.168.1.18  8.8.8.8       DNS               55 Standard query 0x0000 A imgur.com
 29 0.015628  192.168.1.18  192.168.1.1   HTTP              77 GET / HTTP/1.1
 30 0.015628  192.168.1.13  8.8.8.8       DNS               59 Standard query 0x0000 A ads.trackr.io
 31 0.015628  192.168.1.20  8.8.8.8       DNS               67 Standard query 0x0000 A analytics.webdata.com
```

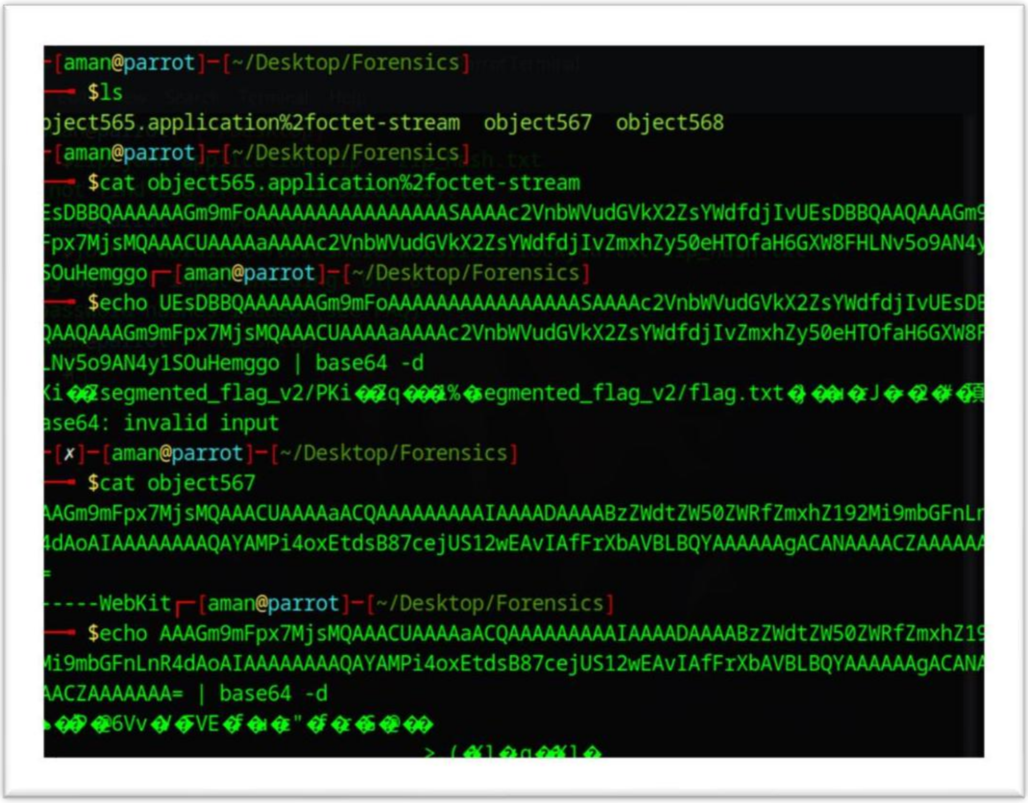
```
Frame 1: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 41929, Dst Port: 53
Domain Name System (query)
```

```
0000  45 00 00 39 00 01 00 00  40 11 a8 ea c0 a8 01 11   E··9····@·······
0010  08 08 08 08 a3 c9 00 35  00 25 d1 4f 00 00 01 00   ·······5·%·O····
0020  00 01 00 00 00 00 00 00  07 74 72 61 63 6b 65 72   ········tracker
0030  03 6c 6f 6c 00 00 01 00  01                        ·lol·····
```

My observation sees it’s as a most of the used protocols are http so I start to check for the http objects to export that.

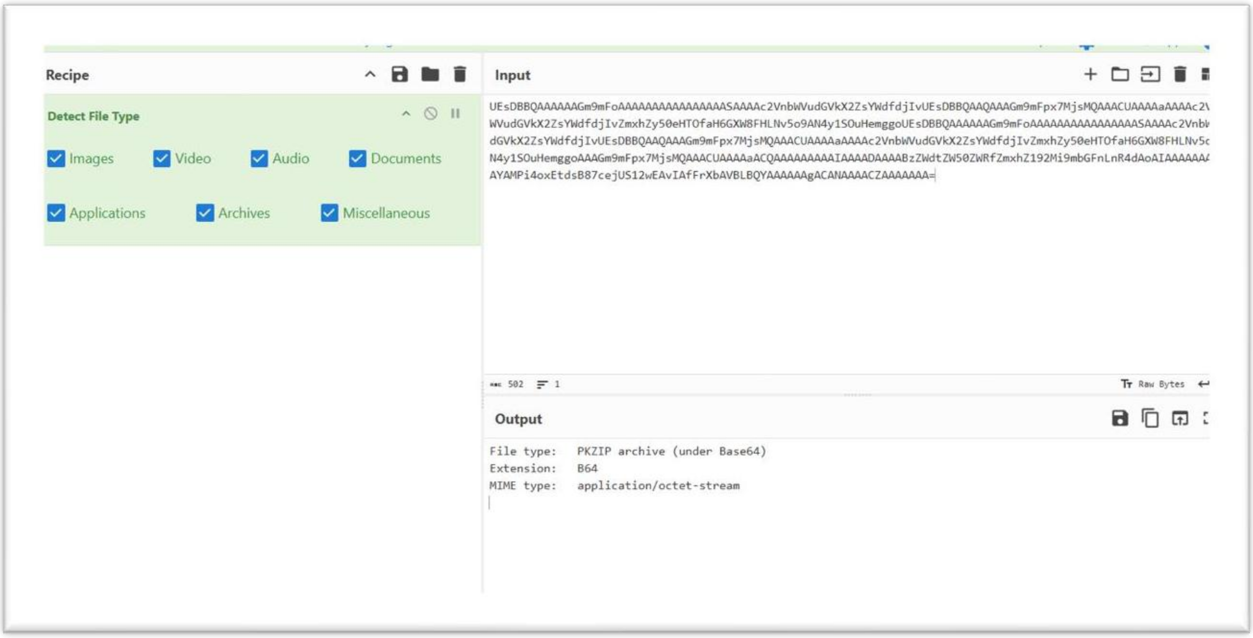


```
Protocol  Length  Info
DNS           57 Standard query 0x0000 A tracker.lol
HTTP          86 GET /graph.png HTTP/1.1
DNS           57 Standard query 0x0000 A tracker.lol
HTTP          87 GET /tracker.js HTTP/1.1
DNS           55 Standard query 0x0000 A imgur.com
DNS           59 Standard query 0x0000 A ads.trackr.io
DNS           59 Standard query 0x0000 A ads.trackr.io
HTTP          87 GET /tracker.js HTTP/1.1
DNS           57 Standard query 0x0000 A tracker.lol
DNS           59 Standard query 0x0000 A ads.trackr.io
HTTP          86 GET /graph.png HTTP/1.1
DNS           55 Standard query 0x0000 A imgur.com
HTTP          86 GET /graph.png HTTP/1.1
DNS           60 Standard query 0x0000 A cdn.google.com
HTTP          86 GET /graph.png HTTP/1.1
DNS           59 Standard query 0x0000 A ads.trackr.io
HTTP          86 GET /graph.png HTTP/1.1
DNS           55 Standard query 0x0000 A imgur.com
DNS           55 Standard query 0x0000 A imgur.com
DNS           55 Standard query 0x0000 A imgur.com
HTTP          80 GET /ads HTTP/1.1
DNS           67 Standard query 0x0000 A analytics.webdata.com
              67 Standard query 0x0000 A analytics.webdata.com
              67 Standard query 0x0000 A analytics.webdata.com
              86 GET /graph.png HTTP/1.1
              57 Standard query 0x0000 A tracker.lol
              90 GET /data/endpoint HTTP/1.1
              55 Standard query 0x0000 A imgur.com
29 0.015628  192.168.1.18  192.168.1.1     77 GET / HTTP/1.1
30 0.015628  192.168.1.13  8.8.8.8         59 Standard query 0x0000 A ads.trackr.io
31 0.015628  192.168.1.20  8.8.8.8         67 Standard query 0x0000 A analytics.webdata.com

Frame 1: 57 bytes on wire (456 bits), 57 bytes captu
Internet Protocol Version 4, Src: 192.168.1.17, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 41929, Dst Port: 53
Domain Name System (query)

0000  45 00 00 39 00 01 00 00  40 11 a8 ea c0 a8 01 11   E··9····@·······
0010  08 08 08 08 a3 c9 00 35  00 25 d1 4f 00 00 01 00   ·······5·%·O····
0020  00 01 00 00 00 00 00 00  07 74 72 61 63 6b 65 72   ·········tracker
0030  03 6c 6f 6c 00 00 01 00  01                        ·lol·····
```



```
-[aman@parrot]-[~/Desktop/Forensics]
──╼ $ls
bject565.application%2foctet-stream  object567  object568
-[aman@parrot]-[~/Desktop/Forensics]
──╼ $cat object565.application%2foctet-stream
EsDBBQAAAAAAGm9mFoAAAAAAAAAAAAAAAAASAAAAc2VnbWVudGVkX2ZsYWdfdjIvUEsDBBQAAQAAAGm9
Fpx7MjsMQAAACUAAAAaAAAAc2VnbWVudGVkX2ZsYWdfdjIvZmxhZy50eHTOfaH6GXW8FHLNv5o9AN4y
SOuHemggo┌─[aman@parrot]-[~/Desktop/Forensics]
──╼ $echo UEsDBBQAAAAAAGm9mFoAAAAAAAAAAAAAAAAASAAAAc2VnbWVudGVkX2ZsYWdfdjIvUEsDB
QAAQAAAGm9mFpx7MjsMQAAACUAAAAaAAAAc2VnbWVudGVkX2ZsYWdfdjIvZmxhZy50eHTOfaH6GXW8F
LNv5o9AN4y1SOuHemggo | base64 -d
Ki��segmented_flag_v2/PKi��q���%�segmented_flag_v2/flag.txt� ��� J� � � �
ase64: invalid input
-[✗]-[aman@parrot]-[~/Desktop/Forensics]
──╼ $cat object567
AAGm9mFpx7MjsMQAAACUAAAAaACQAAAAAAAAAIAAAADAAAABzZWdtZW50ZWRfZmxhZ192Mi9mbGFnLn
4dAoAIAAAAAAAAQAYAMPi4oxEtdsB87cejUS12wEAvIAfFrXbAVBLBQYAAAAAAgACANAAAACZAAAAAA
=
-----WebKit┌─[aman@parrot]-[~/Desktop/Forensics]
──╼ $echo AAAGm9mFpx7MjsMQAAACUAAAAaACQAAAAAAAAAIAAAADAAAABzZWdtZW50ZWRfZmxhZ19
Mi9mbGFnLnR4dAoAIAAAAAAAAQAYAMPi4oxEtdsB87cejUS12wEAvIAfFrXbAVBLBQYAAAAAAgACANA
AACZAAAAAAA= | base64 -d
��@6Vv� �VE� ��"� ���
                         > (�l�g��l�
```

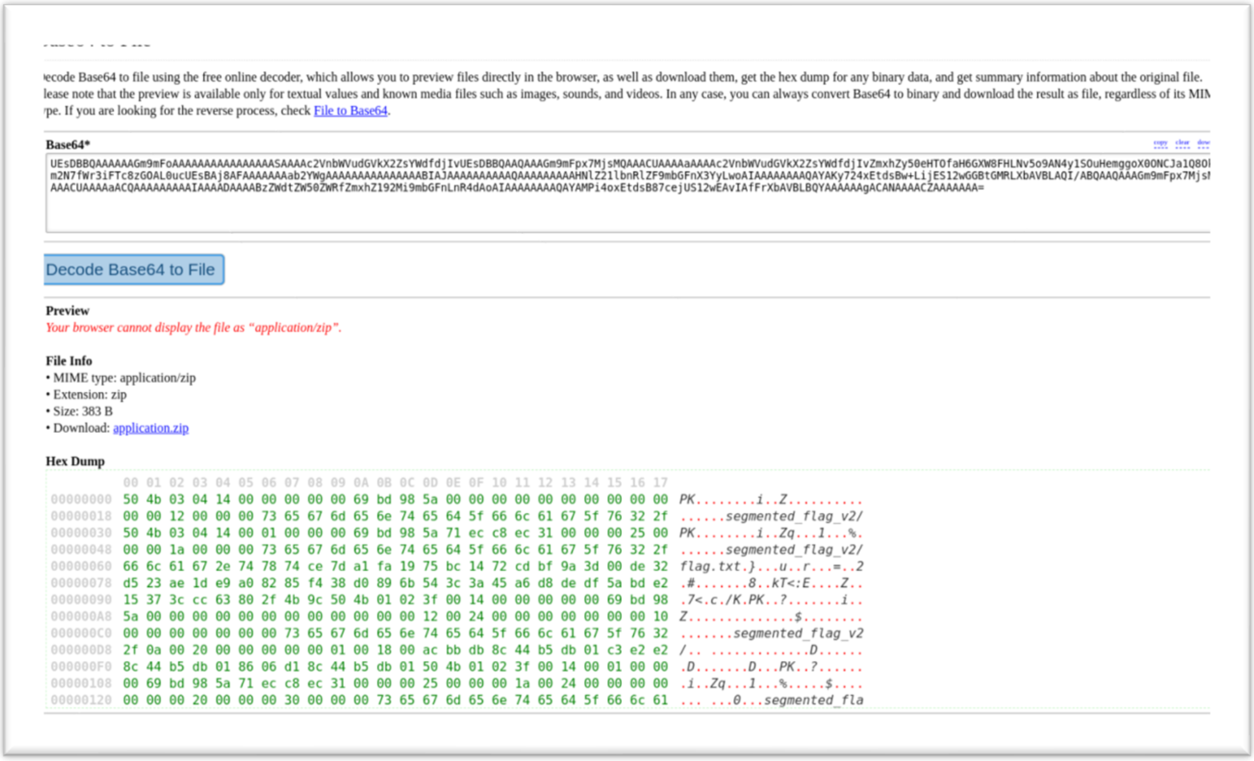
As after seeing all the file, I got the base64 in segments of all the file so I directly go to **Cyberchef** to check it.



UEsDBBQAAAAAAGm9mFoAAAAAAAAAAAAAAAAAASAAAAc2VnbWVudGVkX2ZsYWdfdjIvUEsDBBQAAQAAAGm9mFpx7MjsMQAAACUAAAAaAAAAc2\
WVudGVkX2ZsYWdfdjIvZmxhZy50eHTOfaH6GXW8FHLNv5o9AN4y1SOuHemggoUEsDBBQAAAAAAGm9mFoAAAAAAAAAAAAAAAAAASAAAAc2Vnb
dGVkX2ZsYWdfdjIvUEsDBBQAAQAAAGm9mFpx7MjsMQAAACUAAAAaAAAAc2VnbWVudGVkX2ZsYWdfdjIvZmxhZy50eHTOfaH6GXW8FHLNv5c
N4y1SOuHemggoAAAGm9mFpx7MjsMQAAACUAAAAaACQAAAAAAAAAIAAAADAAAABzZWdtZW50ZWRfZmxhZ192Mi9mbGFnLnR4dAoAIAAAAAA
AYAMPi4oxEtdsB87cejUS12wEAvIAfFrXbAVBLBQYAAAAAAgACANAAAACZAAAAAAA=

```
File type:   PKZIP archive (under Base64)
Extension:   B64
MIME type:   application/octet-stream
```

As its zip archive, I got, so now to download it I use a one decoder tool for the same.



ecode Base64 to file using the free online decoder, which allows you to preview files directly in the browser, as well as download them, get the hex dump for any binary data, and get summary information about the original file. lease note that the preview is available only for textual values and known media files such as images, sounds, and videos. In any case, you can always convert Base64 to binary and download the result as file, regardless of its MIM pe. If you are looking for the reverse process, check File to Base64.

Base64*

UEsDBBQAAAAAAGm9mFoAAAAAAAAAAAAAAAAAASAAAAc2VnbWVudGVkX2ZsYWdfdjIvUEsDBBQAAQAAAGm9mFpx7MjsMQAAACUAAAAaAAAAc2VnbWVudGVkX2ZsYWdfdjIvZmxhZy50eHTOfaH6GXW8FHLNv5o9AN4y1SOuHemggoX0ONCJa1Q80
m2N7fWr3iFTc8zGOAL0ucUEsBAj8AFAAAAAAAab2YWgAAAAAAAAAAAAAAAABIAJAAAAAAAAAAAQAAAAAAAAAAHNlZ21lbnRlZF9mbGFnX3YyLwoAIAAAAAAAAQAYAKy724xEtdsBw+LijES12wGGBtGMRLXbAVBLAQI/ABQAAQAAAGm9mFpx7MjsM
AAACUAAAAaACQAAAAAAAAAIAAAADAAAABzZWdtZW50ZWRfZmxhZ192Mi9mbGFnLnR4dAoAIAAAAAAAAQAYAMPi4oxEtdsB87cejUS12wEAvIAfFrXbAVBLBQYAAAAAAgACANAAAACZAAAAAAA=

Preview

Your browser cannot display the file as "application/zip".

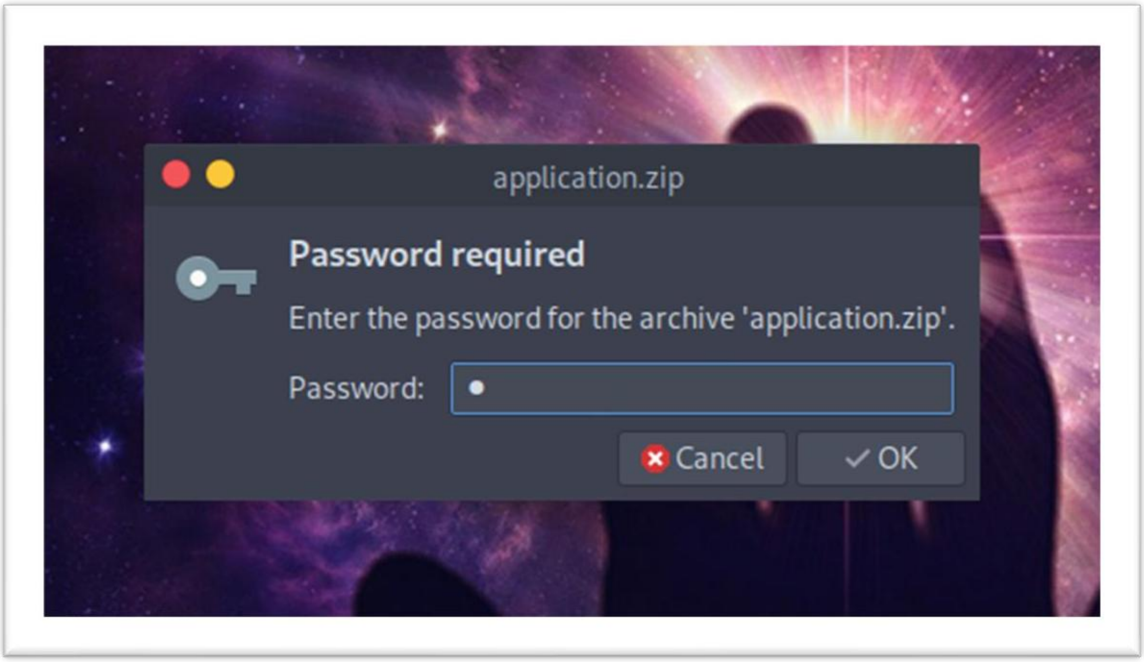
File Info

- MIME type: application/zip
- Extension: zip
- Size: 383 B
- Download: application.zip

Hex Dump

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
00000000  50 4b 03 04 14 00 00 00 00 00 69 bd 98 5a 00 00 00 00 00 00 00 00 00 00  PK........i..Z..........
00000018  00 00 12 00 00 00 73 65 67 6d 65 6e 74 65 64 5f 66 6c 61 67 5f 76 32 2f  ......segmented_flag_v2/
00000030  50 4b 03 04 14 00 01 00 00 00 69 bd 98 5a 71 ec c8 ec 31 00 00 00 25 00  PK........i..Zq...1...%.
00000048  00 00 1a 00 00 00 73 65 67 6d 65 6e 74 65 64 5f 66 6c 61 67 5f 76 32 2f  ......segmented_flag_v2/
00000060  66 6c 61 67 2e 74 78 74 ce 7d a1 fa 19 75 bc 14 72 cd bf 9a 3d 00 de 32  flag.txt.}...u..r...=..2
00000078  d5 23 ae 1d e9 a0 82 85 f4 38 d0 89 6b 54 3c 3a 45 a6 d8 de df 5a bd e2  .#.......8..kT<:E....Z..
00000090  15 37 3c cc 63 80 2f 4b 9c 50 4b 01 02 3f 00 14 00 00 00 00 00 69 bd 98  .7<.c./K.PK..?.......i..
000000A8  5a 00 00 00 00 00 00 00 00 00 00 00 00 12 00 24 00 00 00 00 00 00 00 10  Z.............$.........
000000C0  00 00 00 00 00 00 00 73 65 67 6d 65 6e 74 65 64 5f 66 6c 61 67 5f 76 32  .......segmented_flag_v2
000000D8  2f 0a 00 20 00 00 00 00 00 01 00 18 00 ac bb db 8c 44 b5 db 01 c3 e2 e2  /.. .............D......
000000F0  8c 44 b5 db 01 86 06 d1 8c 44 b5 db 01 50 4b 01 02 3f 00 14 00 01 00 00  .D.......D...PK..?......
00000108  00 69 bd 98 5a 71 ec c8 ec 31 00 00 00 25 00 00 00 1a 00 24 00 00 00 00  .i..Zq...1...%.....$....
00000120  00 00 00 20 00 00 00 30 00 00 00 73 65 67 6d 65 6e 74 65 64 5f 66 6c 61  ... ...0...segmented_fla
```

Now, I downloaded that zip file



application.zip

Password required

Enter the password for the archive 'application.zip'.

Password: ●

As same as rockyou.txt and zip2zohn I got the password as **“letmein”** and got the flag.

FLAG: {multipart_exfiltration_mastered}

~By Team justahacker