Mason CC Advanced Track

Weird Forensics featuring CSAW

Upcoming CTFs

- Capital One
  - Chat me, it's a Tuesday in early October, probably not too late
- CSAW
  - Totally fun
  - Online
  - Part of Cybersecurity Awareness Week
  - No membership limit

Club Updates

- Site updated dramatically
- New logo
- Rooms confirmed
  - See competitivecyber.club
- Most of talks confirmed
  - See competitivecyber.club
  - Paul runs basic track, I run advanced track
  - We get guests
- Booz Allen CTF
- First sponsor approach
  - Ask is $1,000, mainly to cover shirts and CCDC

New Logo

Using Our VM

- If you have our VM, just run **meeting next**

If you don't, **at your own risk (best in Kali)**, do:
curl -s https://competitivecyber.club/commands/next|bash

as root
We aren't responsible if your VM breaks

What are we calling “Forensics”

- “Insert Dictionary.com reference here”

- Looking at files very carefully
  - In unexpected fashion
- Looking at systems very carefully
  - Thoroughly
- **Specifically in a CTF context**

Theory

- Different ways to read data
  - Strings, hex editor, conventional plaintext
  - Encrypted data pulling, e.x. steghide
  - Metadata parsing, more organized
- Often lumped in with steg
- Expect levels of obfuscation

Obscure Problem Examples

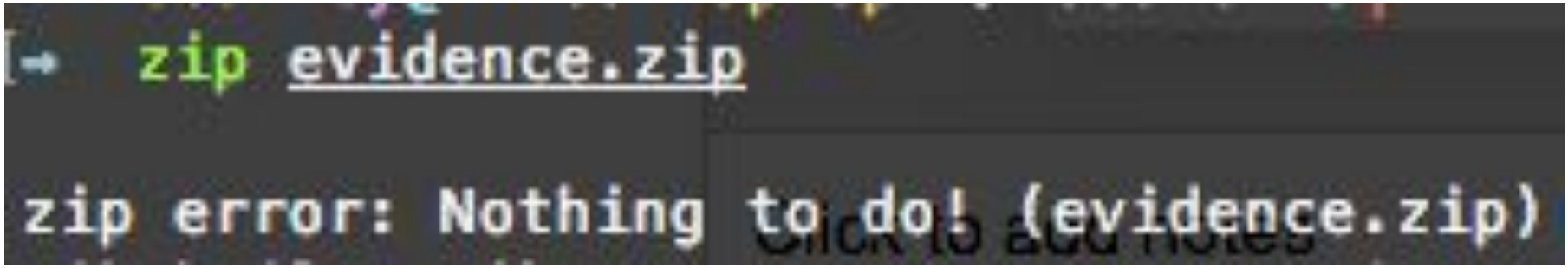
- evidence.zip
  - CSAW 2016
- watchword
  - CSAW 2016
  - High Point Value

evidence.zip

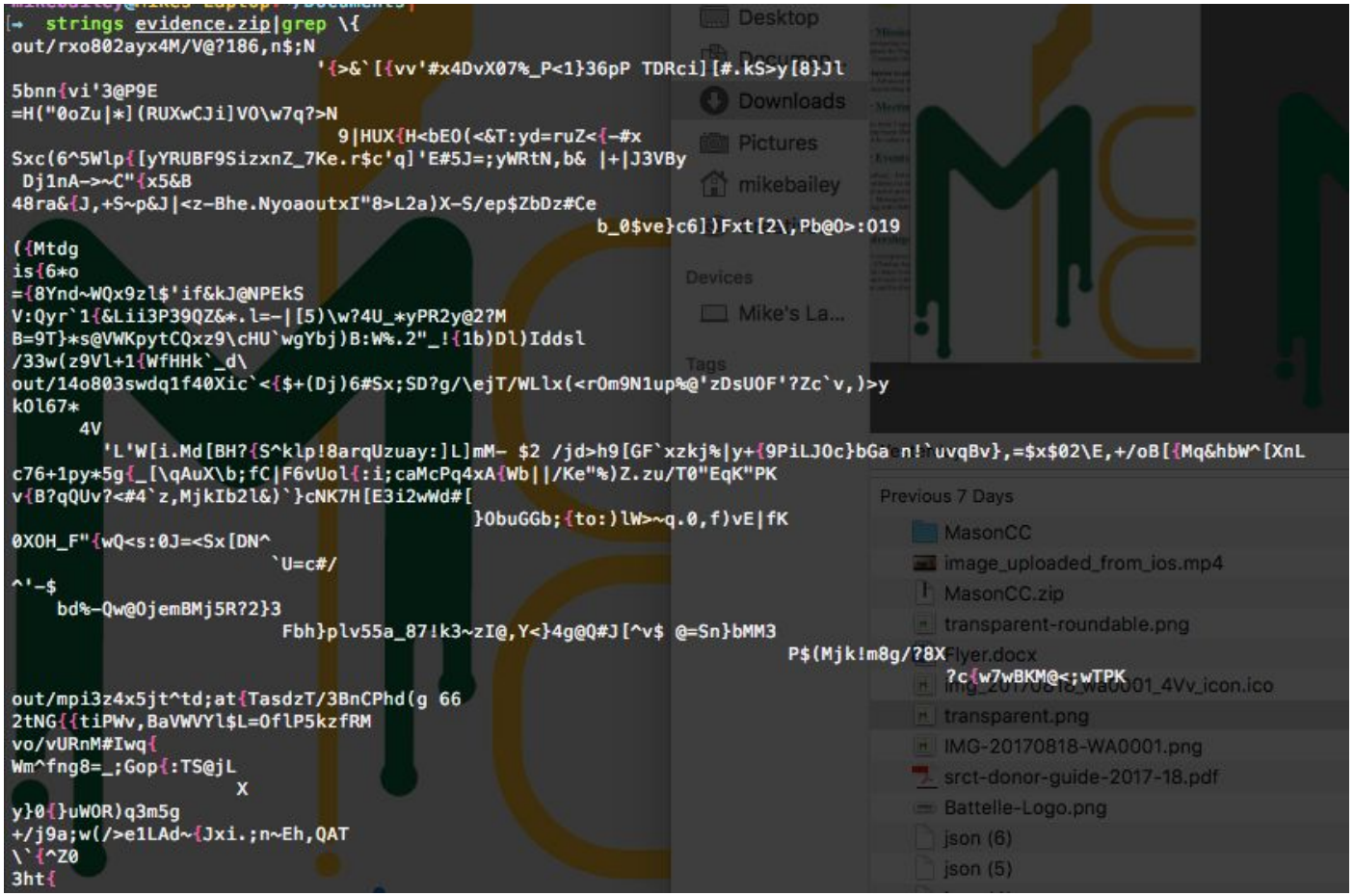
- evidence.zip

“I found this zip file that should have evidence about someone cheating. But for some reason, everything is broken!!”

Next steps?



Strings



No dice, just noise

```
→  strings evidence.zip|grep \{
out/rxo802ayx4M/V@?186,n$;N
                          '{>&`[{vv'#x4DvX07%_P<1}36pP TDRci][#.kS>y[8}Jl
5bnn{vi'3@P9E
=H("0oZu|*](RUXwCJi]VO\w7q?>N
                            9|HUX{H<bEO(<&T:yd=ruZ<{-#x
Sxc(6^5Wlp{[yYRUBF9SizxnZ_7Ke.r$c'q]'E#5J=;yWRtN,b& |+|J3VBy
 Dj1nA->~C"{x5&B
48ra&{J,+S~p&J|<z-Bhe.NyoaoutxI"8>L2a)X-S/ep$ZbDz#Ce
                                                    b_0$ve}c6])Fxt[2\,Pb@O>:O19
({Mtdg
is{6*o
={8Ynd~WQx9zl$'if&kJ@NPEkS
V:Qyr`1{&Lii3P39QZ&*.l=-|[5)\w?4U_*yPR2y@2?M
B=9T}*s@VWKpytCQxz9\cHU`wgYbj)B:W%.2"_!{1b)Dl)Iddsl
/33w(z9Vl+1{WfHHk`_d\
out/14o803swdq1f40Xic`<{$+(Dj)6#Sx;SD?g/\ejT/WLlx(<rOm9N1up%@'zDsUOF'?Zc`v,)>y
kOl67*
      4V
         'L'W[i.Md[BH?{S^klp!8arqUzuay:]L]mM- $2 /jd>h9[GF`xzkj%|y+{9PiLJOc}bGa n!`uvqBv},=$x$02\E,+/oB[{Mq&hbW^[XnL
c76+1py*5g{_[\qAuX\b;fC|F6vUol{:i;caMcPq4xA{Wb||/Ke"%)Z.zu/T0"EqK"PK
v{B?qQUv?<#4`z,MjkIb2l&)`}cNK7H[E3i2wWd#[
                                        }ObuGGb;{to:)lW>~q.0,f)vE|fK
0XOH_F"{wQ<s:0J=<Sx[DN^
                        `U=c#/
^'-$
    bd%-Qw@OjemBMj5R?2}3
                       Fbh}plv55a_87!k3~zI@,Y<}4g@Q#J[^v$ @=Sn}bMM3
                                                          P$(Mjk!m8g/?8X
                                                             ?c{w7wBKM@<;wTPK
out/mpi3z4x5jt^td;at{TasdzT/3BnCPhd(g 66
2tNG{{tiPWv,BaVWVYl$L=OflP5kzfRM
vo/vURnM#Iwq{
Wm^fng8=_;Gop{:TS@jL
                    X
y}0{}uWOR)q3m5g
+/j9a;w(/>e1LAd~{Jxi.;n~Eh,QAT
\`{^Z0
3ht{
```

Metadata

Seems normal...

```
mikebailey@Mikes-Laptop:~/Documents
[→  zipinfo -v evidence.zip
Archive:  evidence.zip
There is no zipfile comment.

End-of-central-directory record:
-------------------------------

  Zip archive file size:                        6680 (0000000000001A18h)
  Actual end-cent-dir record offset:            6658 (0000000000001A02h)
  Expected end-cent-dir record offset:          6658 (0000000000001A02h)
  (based on the length of the central directory and its expected offset)

  This zipfile constitutes the sole disk of a single-part archive; its
  central directory contains 13 entries.
  The central directory is 1040 (000000000000410h) bytes long,
  and its (expected) offset in bytes from the beginning of the zipfile
  is 5618 (00000000000015F2h).


Central directory entry #1:
---------------------------

  out/rxo802ayx4

  offset of local header from start of archive:   0
                                                  (0000000000000000h) bytes
```

Hm....

Suspicious info starts coming up

```
Central directory entry #2:
---------------------------

  There are an extra -20 bytes preceding this file.
```

```
file last modified on (DOS date/time):                  1980 Oct 1
32-bit CRC value (hex):                                 aaaaaaaa
compressed size:                                        485 bytes
```

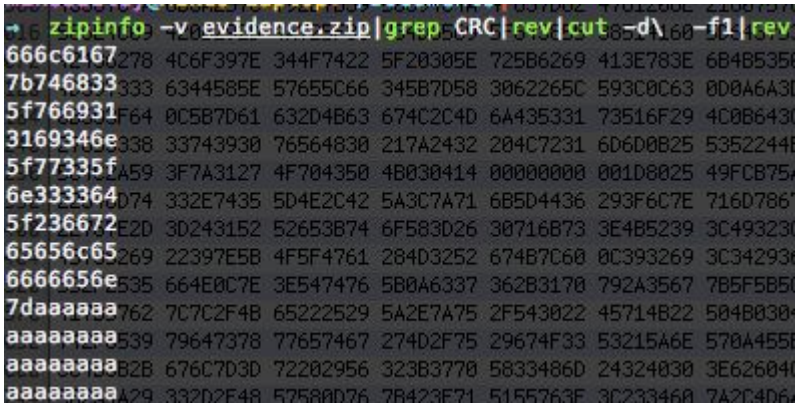
```
zipinfo -v evidence.zip|grep CRC
32-bit CRC value (hex):                                 666c6167
32-bit CRC value (hex):                                 7b746833
32-bit CRC value (hex):                                 5f766931
32-bit CRC value (hex):                                 3169346e
32-bit CRC value (hex):                                 5f77335f
32-bit CRC value (hex):                                 6e333364
32-bit CRC value (hex):                                 5f236672
32-bit CRC value (hex):                                 65656c65
32-bit CRC value (hex):                                 6666656e
32-bit CRC value (hex):                                 7daaaaaa
32-bit CRC value (hex):                                 aaaaaaaa
32-bit CRC value (hex):                                 aaaaaaaa
32-bit CRC value (hex):                                 aaaaaaaa
```

Now what?

- There were two valid solve strategies
  - One is cleaner, both fast

- Guess the answer

Pull CRCs, concat



zipinfo CRCs...

```
→ zipinfo -v evidence.zip|grep CRC|rev|cut -d\ -f1|rev
666c6167
7b746833
5f766931
3169346e
5f77335f
6e333364
5f236672
65656c65
6666656e
7daaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
```

zipinfo -v evidence.zip|grep CRC|rev|cut -d\ -f1|rev|xargs -I% echo -n %

```
→ zipinfo -v evidence.zip|grep CRC|rev|cut -d\ -f1|rev|xargs -I% echo -n %
666c61677b7468335f7669313169346e5f77335f6e3333645f23667265656c656666656e7daaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

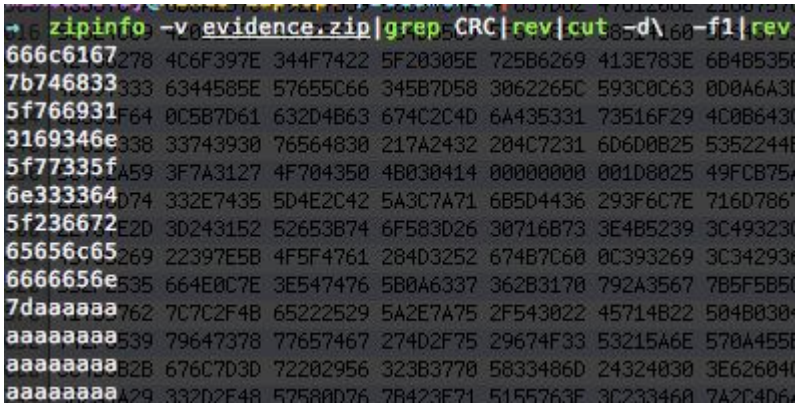
Cleaned input:

666C61677B7468335F7669313169346E5F77335F6E3333645F2366

Decoded data as ASCII text, bytes outside 32...126 range

flag{th3_vi1li4n_w3_n33d_#freeleffen}*[170][*

Pull CRCs, concat



zipinfo CRCs...

```
→ zipinfo -v evidence.zip|grep CRC|rev|cut -d\ -f1|rev
666c6167
7b746833
5f766931
3169346e
5f77335f
6e333364
5f236672
65656c65
6666656e
7daaaaaa
aaaaaaaa
aaaaaaaa
aaaaaaaa
```

zipinfo -v evidence.zip|grep CRC|rev|cut -d\ -f1|rev|xargs -I% echo -n %

```
→ zipinfo -v evidence.zip|grep CRC|rev|cut -d\ -f1|rev|xargs -I% echo -n %
666c61677b7468335f7669313169346e5f77335f6e3333645f23667265656c656666656e7daaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Cleaned input:

666C61677B7468335F7669313169346E5F77335F6E3333645F2366

Decoded data as ASCII text, bytes outside 32...126 range

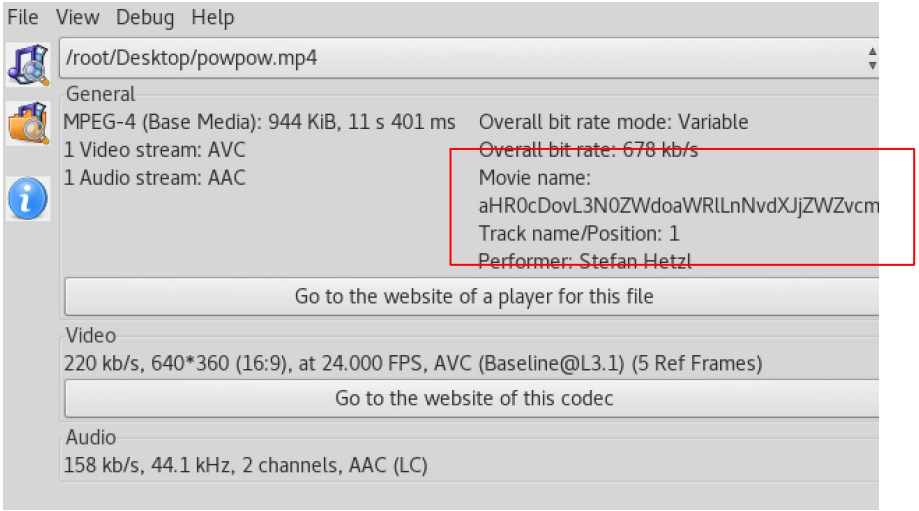
flag{th3_vi1li4n_w3_n33d_#freeleffen}*[170][*

Watchword - 250

- Watchword - synonym for password
- CSAW 2016 major problem
- provided **powpow.mp4**

Pretty Much Immediately

- Pretty much immediate metadata fun with either **exiftool** or **mediainfo** you find the title is base64




```
root@ccvm:~/Desktop# echo -n aHR0cDovL3N0ZWdoaWRlLnNvdXJjZWZv
cmdlLm5ldC8=|base64 --decode
http://steghide.sourceforge.net/root@ccvm:~/Desktop#
```

So that's a gimme...

- Steghide supports JPGs
- **foremost powpow.mp4**

```
root@ccvm:~/Desktop# foremost powpow.mp4
Processing: powpow.mp4
|*|
root@ccvm:~/Desktop# ls
output  powpow.mp4
root@ccvm:~/Desktop# cd output/
root@ccvm:~/Desktop/output# ls
audit.txt  mov  png
root@ccvm:~/Desktop/output# cd png
root@ccvm:~/Desktop/output/png# ls
00001069.png
```

Ok… now what?

- **I couldn’t just use the *convert* command**
- Was apparently stripping key data?
- Used **stepic**

```
root@ccvm:~/Desktop/output/png# stepic -d -i 00001069.png > f
orensic.png
```

Steghide with the password “password” revealed base64.txt

Now...?

- I couldn't just use the *convert* command
- Was apparently stripping key data?
- Used stepic

```
root@ccvm:~/Desktop/output/png# stepic -d -i 00001069.png > f
orensic.png
```

Steghide with the password "password" revealed base64.txt

Too many chars...

Key bit here: the character set is too wide to be b64

Bigger base: base85?

Failed, strip, try again

```
ValueError: bad base85 character at position 82
>>> base64.b85decode(open('base64.txt').readlines()[0].strip())
b'flag{We are fsociety, we are finally free, we are finally awa
ke!}'
>>>
```

Bonus as needed:

ransomwhere

https://github.com/krx/CTF-Writeups/tree/master/CSAW%2015%20Finals/for300%20-%20randsomewhere

Bonus as needed:

ransomwhere

https://github.com/krx/CTF-Writeups/tree/master/CSAW%2015%20Finals/for300%20-%20randsomewhere