Conference d'ouverture
[titre à venir]

Travis Goodspeed

4 June 2014
SSTIC
Rennes, Bretagne, France

Prezegenn digeriñ
[titl da zont]

Travis Goodspeed

4 June 2014
SSTIC
Roazhon, Breizh

GOOD MORNING!

GOOD MORNING!

- I hate keynotes.
  - (Except those by Fx and Dan Geer.)
- I love proofs of concept.
  - Short, nifty tricks.
  - No grand theories, no unnecessary tables.

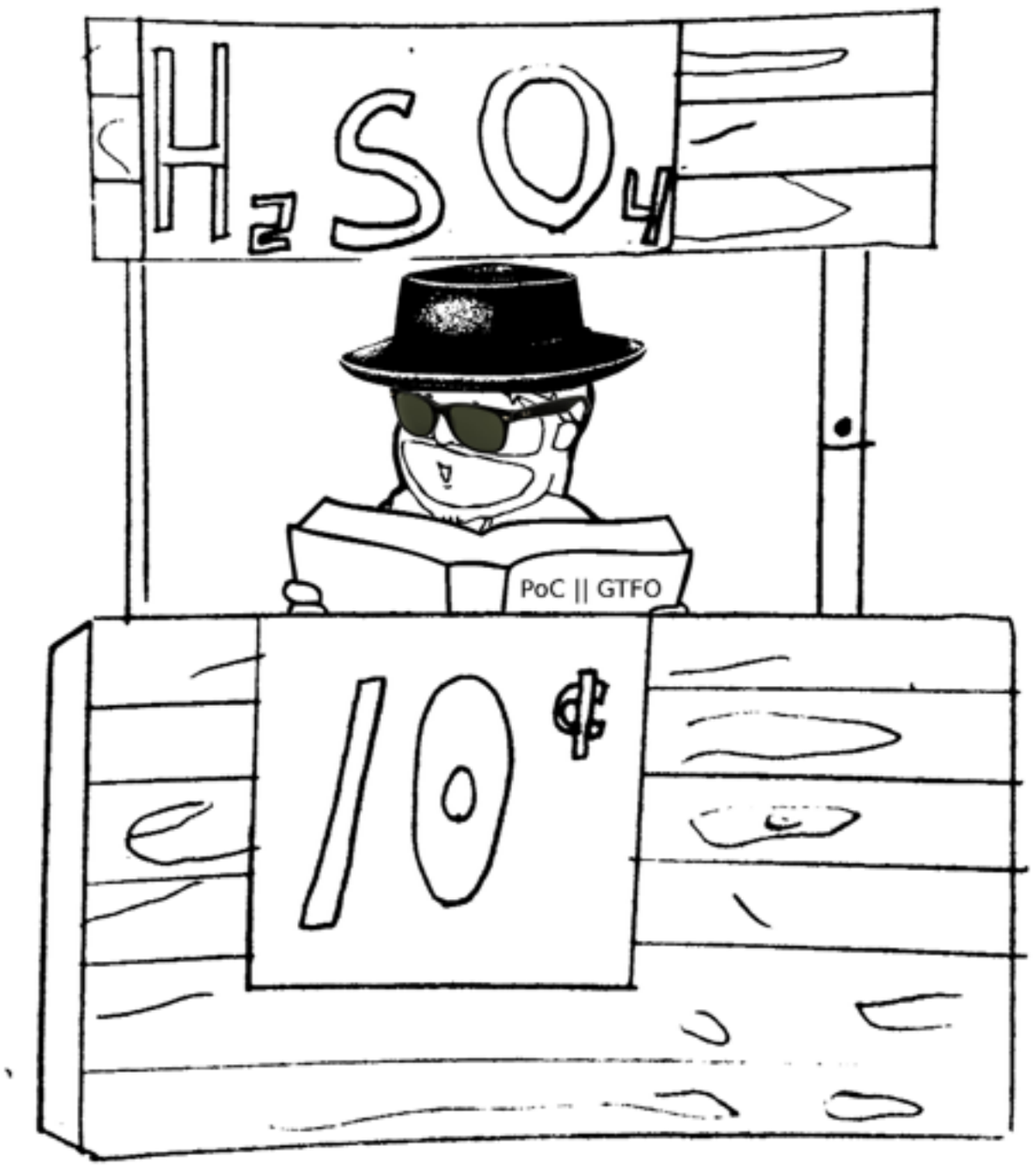
Proofs of Concept are Proofs by Construction

Proofs of Concept
are
Proofs by Construction

by Travis Goodspeed
to them Ghosts who write History Books
and the Ghosts in my Drink
concerning the Good Works
and the Good Neighbors
of PoC||GTFO.

4 June 2014
SSTIC
Rennes, Brittany, France

Did you know that you can just start a journal?



Did you know that you can just start a journal?

- A neighbor and I started a journal.
- No peer review, just a benevolent dictatorship.
    - Pastor Manul Laphroaig, Amateur Tyrant

International Journal of PoC || GTFO
Issue 0x00, a CFP with PoC

An epistle from the desk of Rt. Revd. Pastor Manul Laphroaig
pastor@phrack.org

August 5, 2013

Proceedings of the Society of PoC || GTFO
Issue 0x01, an Epistle to the 10th H2HC in São Paulo

From the writing desk, not the raven, of Rt. Revd. Preacherman Pastor Manul Laphroaig
pastor@phrack.org

Children's Bible Coloring Book of PoC || GTFO
Issue 0x02, an Epistle to the 30th CCC Congress in Hamburg

Composed by the Rt. Revd. Pastor Manul Laphroaig to put pwnage before politics.
pastor@phrack.org

December 28, 2013

AN ADDRESS
to the
SECRET SOCIETY
of
POC || GTFO
concerning
THE GOSPEL OF THE WEIRD MACHINES
and also
THE SMASHING OF IDOLS TO BITS AND BYTES
by the Rt. Revd. Dr.
PASTOR MANUL LAPHROAIG

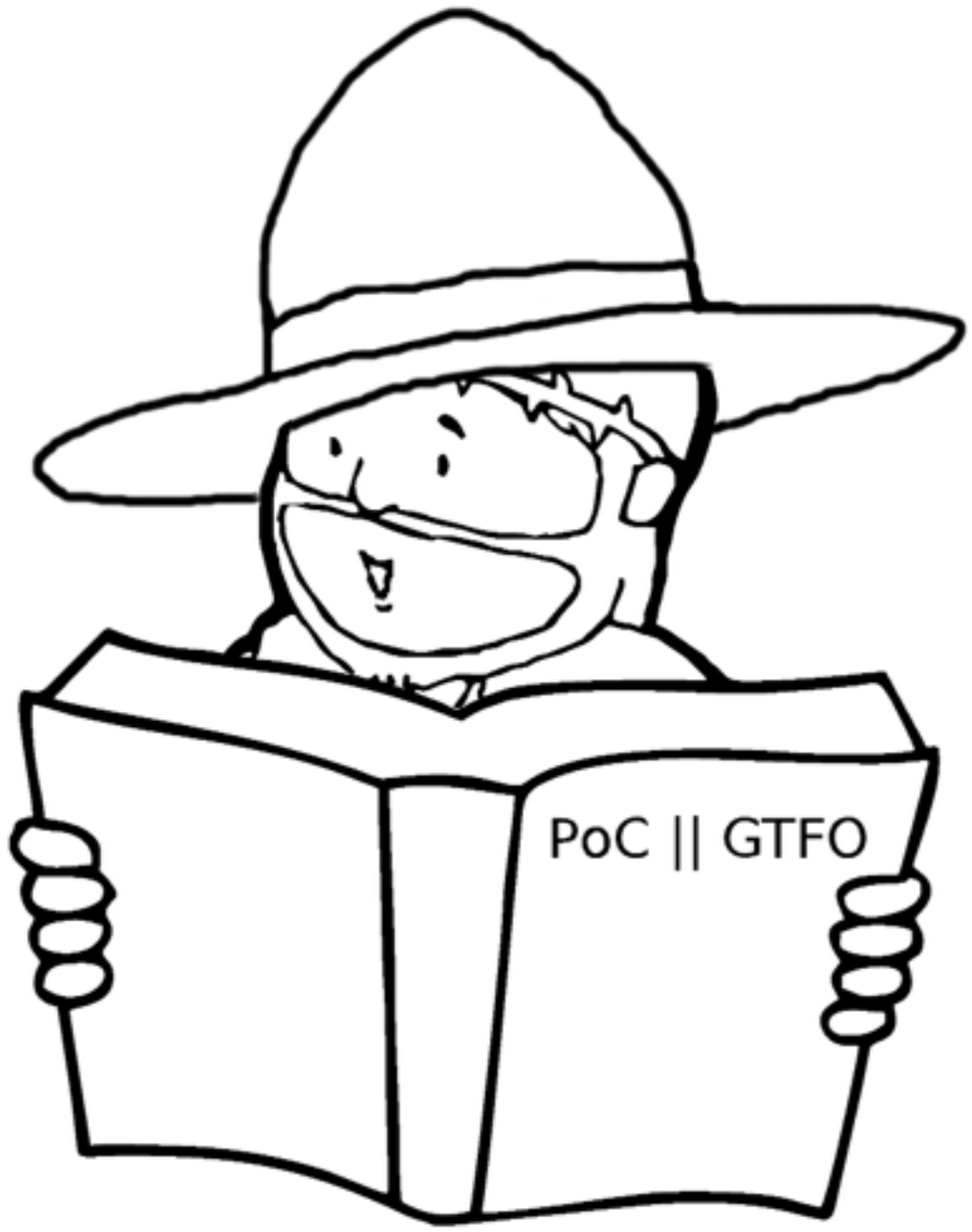
pastor@phrack.org

TRACT
de la
SOCIÉTÉ SECRÈTE
de
POC || GTFO
sur
L'EVANGILE DES MACHINES ETRANGES
et autres
SUJETS TECHNIQUES
par le prédicateur

PASTEUR MANUL LAPHROAIG

pastor@phrack.org

Let’s hear some stories!



Nifty Tricks for Today

- Active Disk Antiforensics
- PGP Matryoshka Doll
- PDF+Zip Polyglot
- Angecryption
- Strange Python Encodings

Active Disk Antiforensics
PoC||GTFO 0:2

Active Disk Antiforensics

- You think of a disk as a block device.
    - Blocks are written, then read back intact.
    - Sometimes they are damaged.
- A disk is really a server.
    - Host makes requests by SCSI or ATA.
    - Software in the disk responds.


Demotivation.us
novate.ru


novate.ru

iPod is a Computer

- Low-end ARM with hardware MP3 decoding.
- Custom operating systems
  - iPod Linux, Rockbox
- Disk Mode is implemented in software.
  - C code translates USB Mass Storage to ATA.

iPod Disk Layout

- First sector is MBR.
- Then comes the iPod Firmware.
- Finally, there is a FAT32 or HFS+ partition for music.

iPod Disk Layout

This is *NEVER* legitimately read by the host!

- First sector is MBR.
- Then comes the iPod Firmware.
- Finally, there is a FAT32 or HFS+ partition for music.

Fingerprinting a Host OS

- Windows
  Reads the Master Boot Record (MBR) 9 times.

- FreeBSD
  Speaks some antique SCSI requests.

- OpenBSD
  Doesn’t delay on SCSI errors.

- Linux
  Varies by automounter.

Fingerprinting Disk Imaging

- tar -cf mnt.tar /mnt
  Follows the filesystem structures,
  never reading empty space,
  or deleted files, or orphaned inodes.

- dd if=/dev/sdc of=forensics.img
  This reads from the beginning to the end,
  in order, as large blocks, without reading ahead,
  and without following filesystem or partition structs.

So let's make a trap!

- Pick an unused sector early in the disk.
- The sector must be one that is *NEVER* read.
- If this sector is read anyways,
  - Erase all future sectors.
  - Reply with legitimate-looking garbage.

Disk Imaging my iPod

```
//These sectors are for 2048-byte sectors.
//Multiply by 4 for devices with 512-byte sectors.
if(cur_cmd.sector>=10000 && cur_cmd.sector<48000)
  tamperdetected=true;
```

Terminal

File Edit View Search Terminal Help

```
0555c000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 6c 65 74 20  |Never gonna let |
0555c010  79 6f 75 20 64 6f 77 6e  2e 00 ff ff ff ff ff ff  |you down.....|
0555c020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
0556c000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 67 69 76 65  |Never gonna give|
0556c010  20 79 6f 75 20 75 70 2e  00 ff ff ff ff ff ff ff  | you up.....|
0556c020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
0557a000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 6c 65 74 20  |Never gonna let |
0557a010  79 6f 75 20 64 6f 77 6e  2e 00 ff ff ff ff ff ff  |you down.....|
0557a020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
0558a000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 67 69 76 65  |Never gonna give|
0558a010  20 79 6f 75 20 75 70 2e  00 ff ff ff ff ff ff ff  | you up.....|
0558a020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
05598000  4e 65 76 65 72 20 67 6f  6e 6e 61 20 6c 65 74 20  |Never gonna let |
05598010  79 6f 75 20 64 6f 77 6e  2e 00 ff ff ff ff ff ff  |you down.....|
05598020  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
```

Beyond a PoC

- ACSAC 2014, Seagate Disk Backdoor
  - Talk to Aurélien Francillon. He's here!
- Sprites Mods, Western Digital Reverse Engineering
  - He booted Linux on a WD hard disk!

Myron Aub's
PGP Matryoshka Doll

PoC||GTFO 2:3

PGP Matryoshka Doll

- RFC 4880, `OpenPGP Message Format'
  by Phil Zimmerman

- Messages are compressed or encrypted.
  - These are just containers, and they can be nested!
  - You can required more than one key for decrypt.
  - You can compress more than once.

Lempel-Ziv (LZ) Compression

- A dictionary is used as shorthand for a larger file.

- The output of the decompression can be the same as the input.

PGP Quine

- Message, when decompressed, is itself.
- After decompression, the parser tries to go deeper.
  - And deeper.
    - And deeper.
      - And deeper!

PGP Quine

```
a0 b0 01 00 03 00 fc ff  a0 b0 01 00 0d 00 f2 ff  |................|
00 03 00 fc ff a0 b0 01  00 0d 00 f2 ff 82 70 a0  |..............p.|
1c 00 00 05 00 fa ff 82  70 a0 1c 00 00 05 00 fa  |........p.......|
ff 00 05 00 fa ff 00 14  00 eb ff 82 70 a0 1c 00  |............p...|
00 05 00 fa ff 00 05 00  fa ff 00 14 00 eb ff 42  |...............B|
88 21 c4 00 00 14 00 eb  ff 42 88 21 c4 00 00 14  |.!.......B.!....|
00 eb ff 42 88 21 c4 00  00 14 00 eb ff 42 88 21  |...B.!.......B.!|
c4 00 00 14 00 eb ff 42  88 21 c4 00 00 00 00 ff  |.......B.!......|
ff 00 00 00 ff ff 00 0a  00 f5 ff 42 88 21 c4 00  |...........B.!..|
00 00 00 ff ff 00 00 00  ff ff 00 0a 00 f5 ff 02  |................|
b3 c0 2c 40 00 00 00 ff  ff 02 b3 c0 2c 40 00 00  |..,@........,@..|
00 ff ff                                         |...|
```

- GnuPG fixed this bug.
- Symantec PGP didn’t fix this bug.

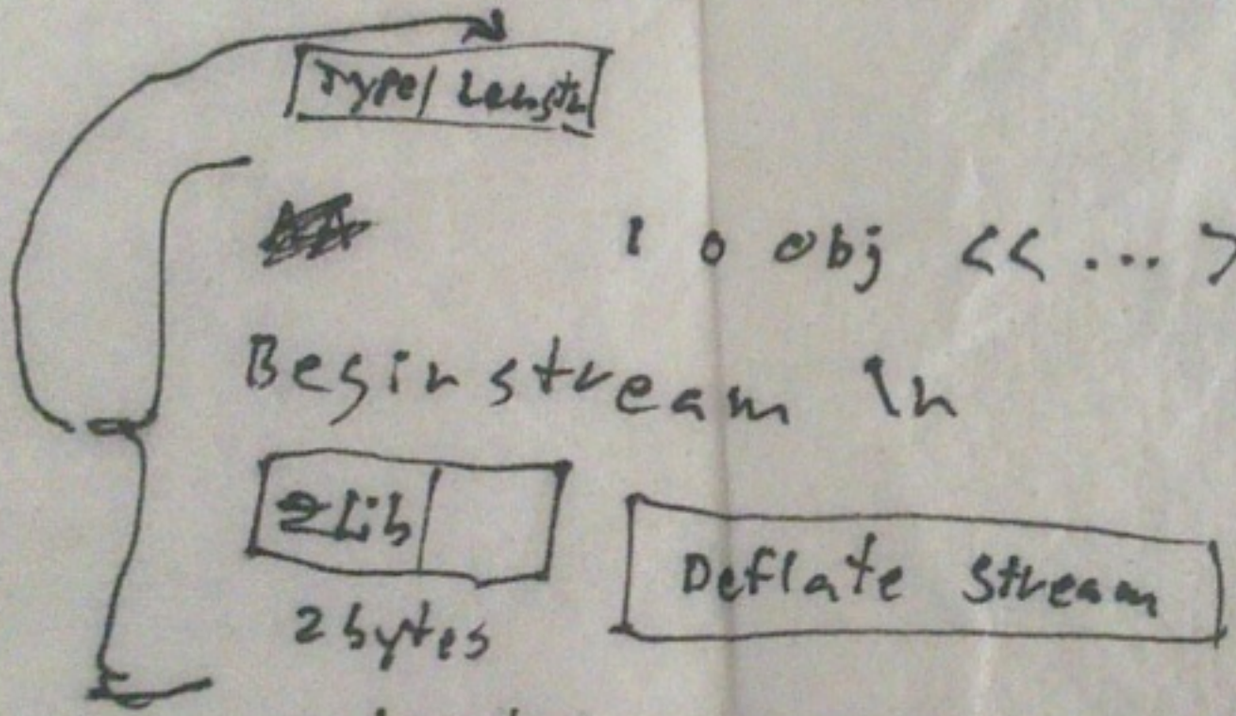
PDF that's a ZIP File
PoC||GTFO 1:5

- Zip files begin with a footer near the end of a file.
- This makes them easy to combine with other files.
  - cat foo.gif foo.zip >zipgif.bin
- PDF also ends near the end.

% PDF-1.etc \n

% PK \003 \004 etc... Not CR, LF, or NUL

Zip Metadata



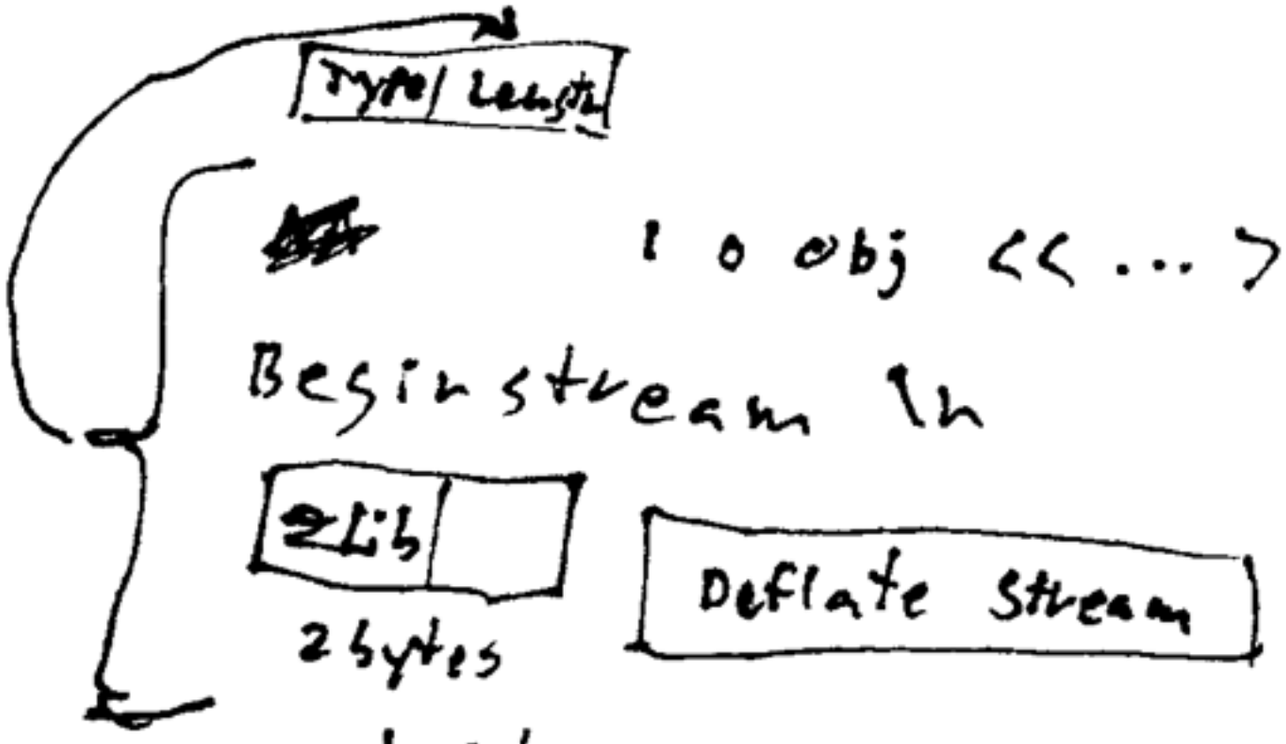
% PK \003 \004 (See above)

(Repeat)

% PDF-1.etc \n

% PK \003 \004 etc... Not CR, LF, or NUL

Zip metadata



end stream

end obj

% PK \003 \004 (See above)

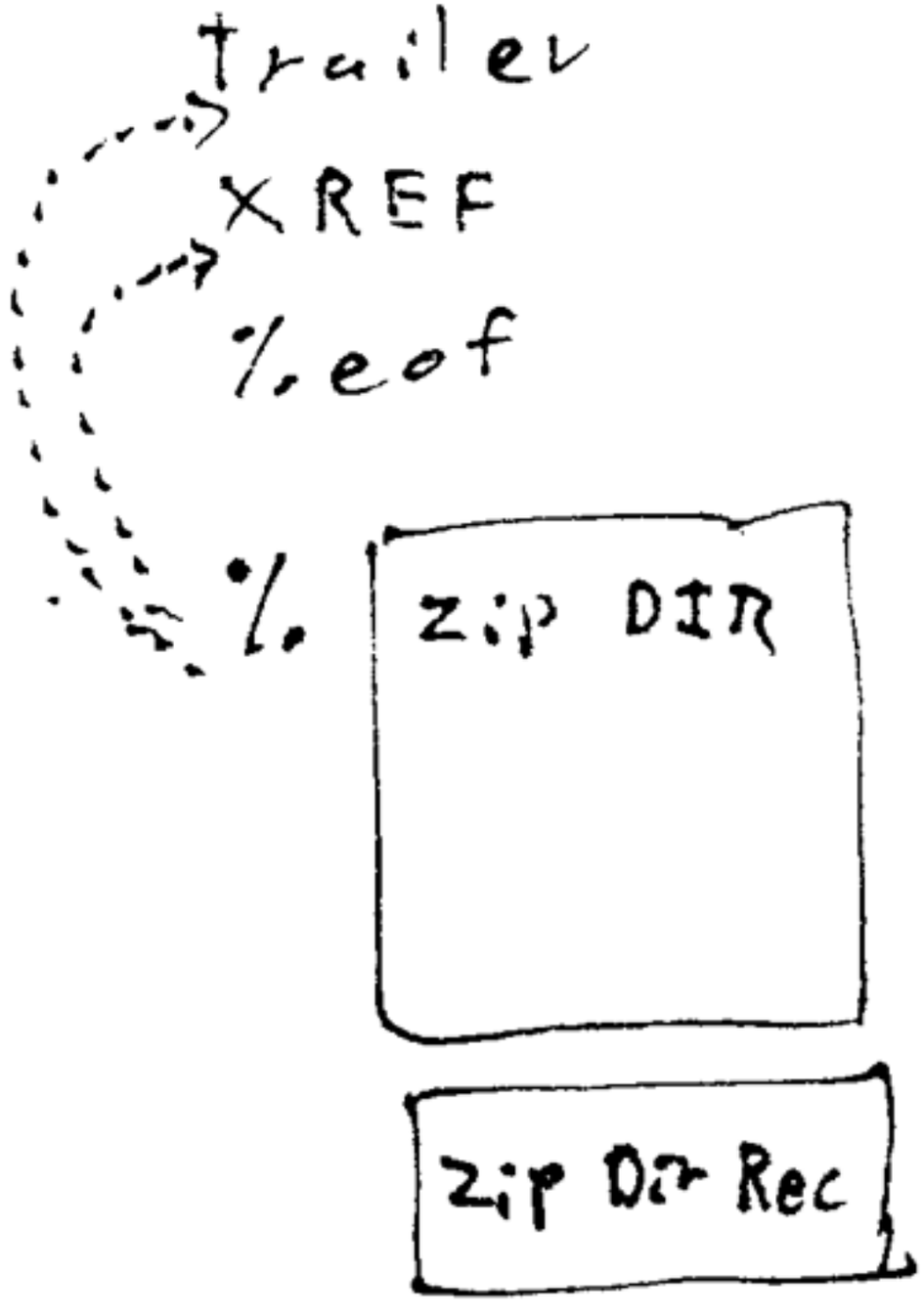
(Repeat)

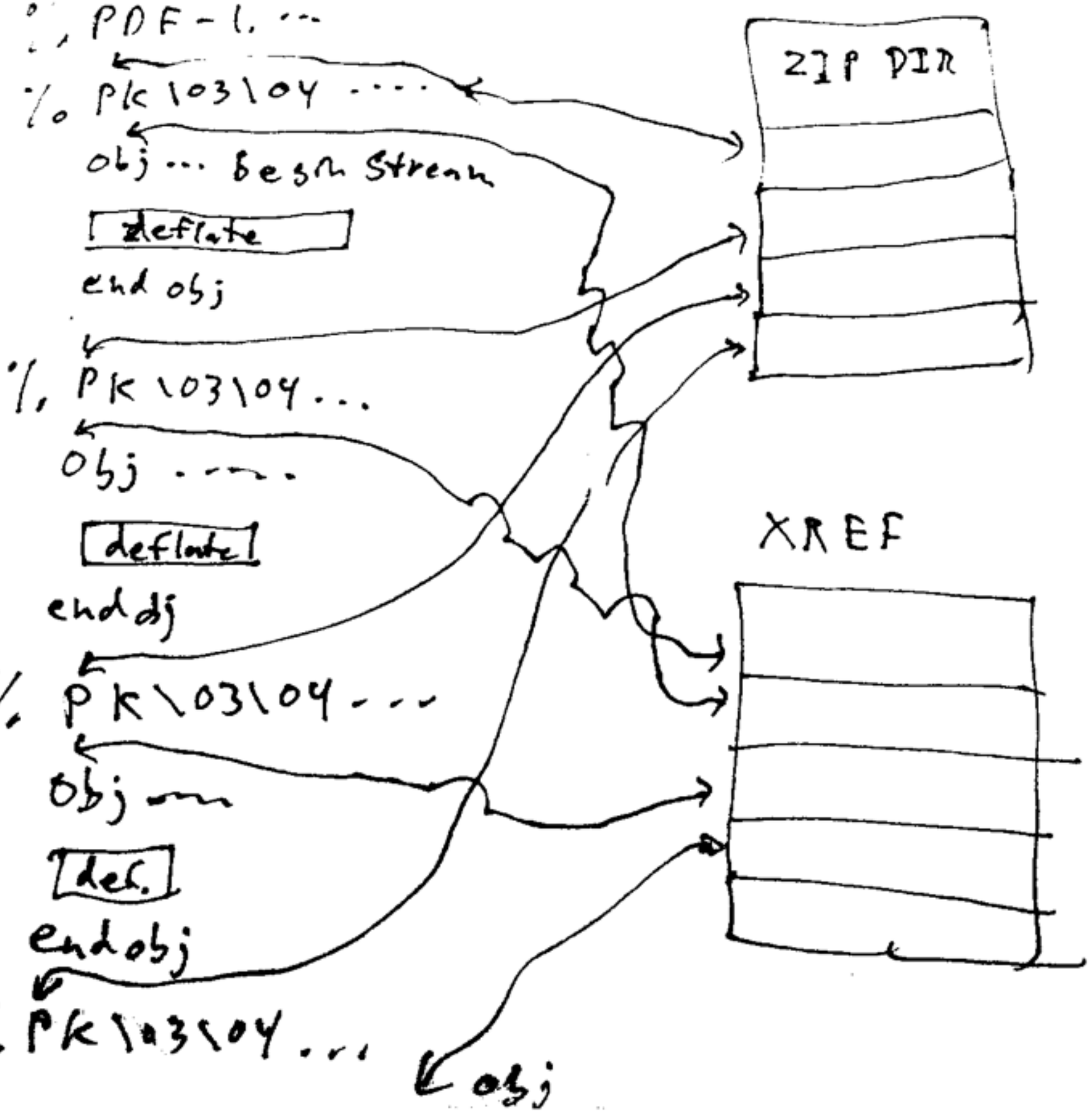
END

OPTION 1

Probably Best ↙

OPTION 2




%PDF-1. ...
%PK\03\04 ....
obj ... begin Stream
[deflate]
end obj
%PK\03\04...
Obj ....
[deflate]
end obj
%PK\03\04...
Obj ...
[def.]
endobj
%PK\03\04...
Obj
ZIP DIR
XREF

cat foo.pdf bar.zip > buz.pdf

zip -A buz.pdf

or...

cat foo.pdf bar.zip foo.pdf > buz.pdf

zip -A buz.pdf

Or...

echo -e "trailer <</root/... >>\n xref \n ..... etc. %%EOF" > comment.txt

cat foo.pdf bar.zip > bbz.pdf

zip -z comment.txt ~~bar.zip~~ ~~-A buz.pdf~~ stuff

cat

zip -A buz.pdf

PDF+ZIP

- For very small Zips, just
  cat foo.pdf foo.zip >bar.pdf

- For larger files, insert the zip just before the PDF's closing xref table.

- This is reliable, and we've shipped it in every release since the first.

Angecryption
PoC||GTFO 3:11

Ange Albertini
Jean-Philippe Aumasson

Angecryption

- pocorgtfo03.pdf was a valid PDF file.
- Encrypt it with AES CBC to get a valid PNG file.
  key=“Manul Laphroaig!”
  IV=5B F0 15 E2 04 8C E3 D3 8C 3A 97 E7 8B 79 5B C1
- Ain’t that nifty?

Angecryption

- It's easy to control ECB-mode data before or after encryption.
  - AES(controlled)=uncontrolled
  - controlled=AES(uncontrolled)
    AES^-1(controlled)=uncontrolled
- Angecryption lets us make a file valid before and after encryption, with different contents!

The Nifty Trick

- In ECB mode, we control each block before or after encryption.
- In CBC mode, the same is true, *except*
  - The very first block is XOR'ed with the IV,
  - and we control the IV, so
  - we control Block 0 before *and after* encryption!

Weird Python Encoding PoC||GTFO 3:10

Frederik Baun

```
% cat poc.py
#! /usr/bin/python
#encoding: rot13
cevag 'Hello World'
% ./poc.py
Hello World
%
```

Proofs of Concept are Proofs by Construction

Proof of Concept is Proof by Construction

- A proof by construction is the best kind of proof.
  - See Euclid's proof that there are infinitely many prime numbers.
- Stop calling them unscientific!
  Stop demanding statistics!
- ``You can't argue with a root shell.''

Go now in peace.

- Read your scripture.
  - PoC||GTFO, Phrack, and SSTIC proceedings!
- Preach the good news!
  - Conference talks, soap box.
  - ``Hey, want to learn a cool trick?''

Credits

- Antiforensic iPod, PoC||GTFO 0:2
  Travis Goodspeed

- PGP Matryoshka, PoC||GTFO 2:3
  Myron Aub

- PDF Zip File, PoC||GTFO 1:5
  Julia Wolf

- Angecryption, PoC||GTFO 3:11
  Ange Albertini
  Jean-Philippe Aumasson

- Weird Python Encoding, PoC||GTFO 3:10
  Frederik Braun