File Polyglottery

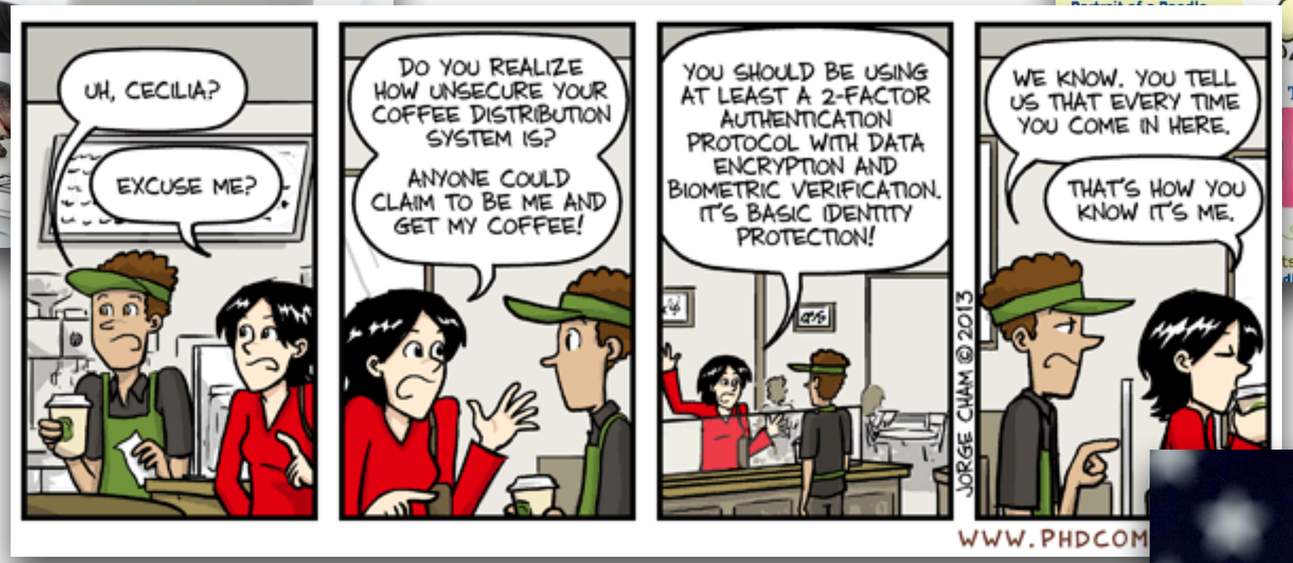
or, This Proof of Concept is Also a Picture of Cats

Evan Sultanik

https://www.sultanik.com/

@ESultanik

`whoami`



APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

DigitalOperatives

TRAIL OF BITS

Drexel UNIVERSITY

PoC*or*GTFO

Proof of Concept

(Pictures of Cats)

"It looks great on a shelf, and if you read PoC||GTFO on public transportation, people stay away from you."

—Hackaday Review

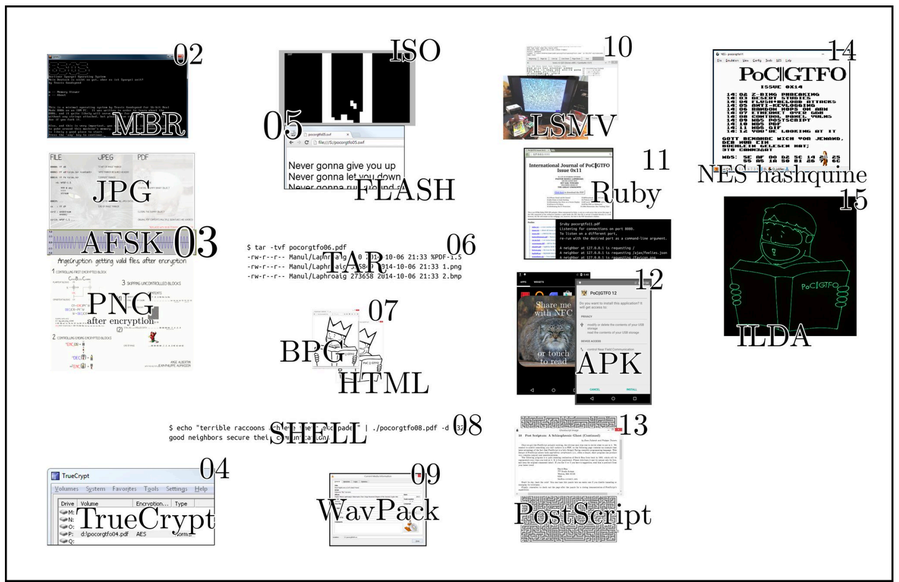
Roughly quarterly journal, in the tradition of Phrack and Uninformed

Offensive security research and stunt hacking

Issue 0x17 will be released at CCC

First released on paper at a conference, later released digitally

Each digital release is a Polyglot



Neil Madden @neilmaddog · Jul 19

I wonder what happened to PoC||GTFO issues 0x0A–0x0F…

1

Evan Sultanik

@ESultanik

Replying to @neilmaddog

We number in BCD in honor of the HP48 calculator's floating point implementation, which matches decimal rounding errors.

3:01 PM - 19 Jul 2017

`https://sultanik.com/pocorgtfo/`

PoC*or*GTFO

Proof of Concept

(Pictures of Cats)

"It looks great on a shelf, and if you read PoC||GTFO on public transportation, people stay away from you."

—Hackaday Review

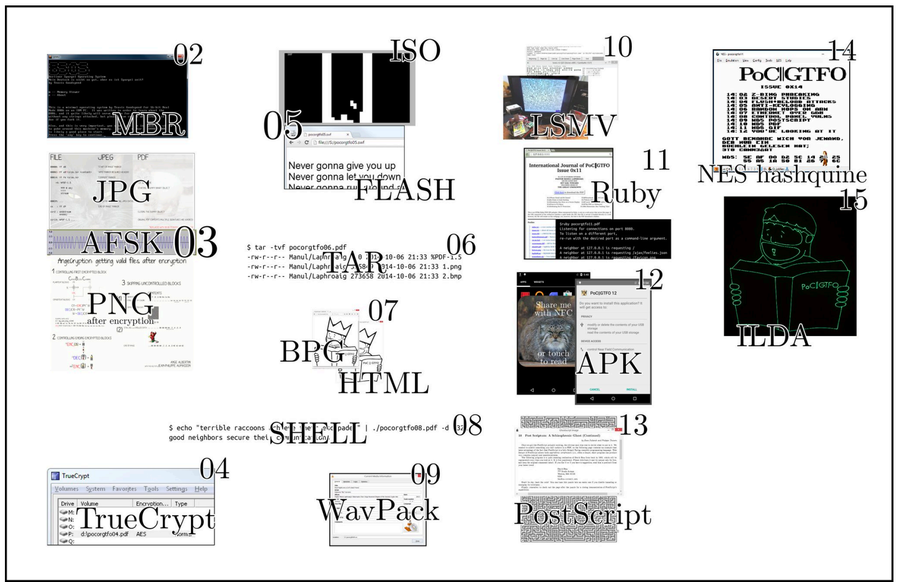
Roughly quarterly journal, in the tradition of Phrack and Uninformed

Offensive security research and stunt hacking

Issue 0x17 will be released at CCC

First released on paper at a conference, later released digitally

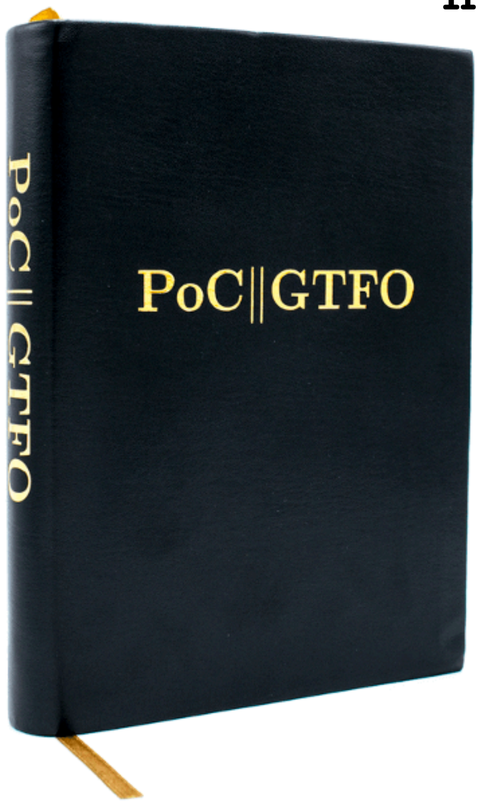
Each digital release is a Polyglot

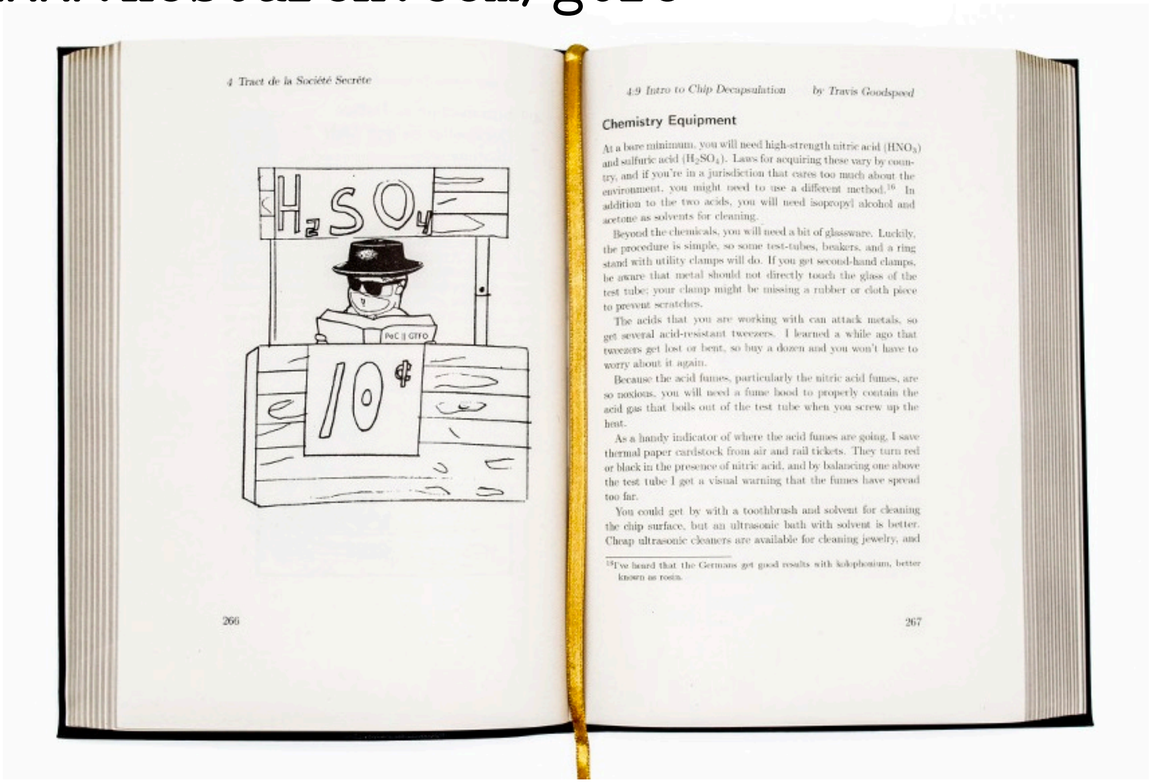


https://sultanik.com/pocorgtfo/

The Book of PoC||GTFO

https://www.nostarch.com/gtfo





"...a file has no intrinsic meaning. The meaning of a file—its type, its validity, its contents—can be different for each parser or interpreter"

—PoC||GTFO 7:6 by Ange Albertini

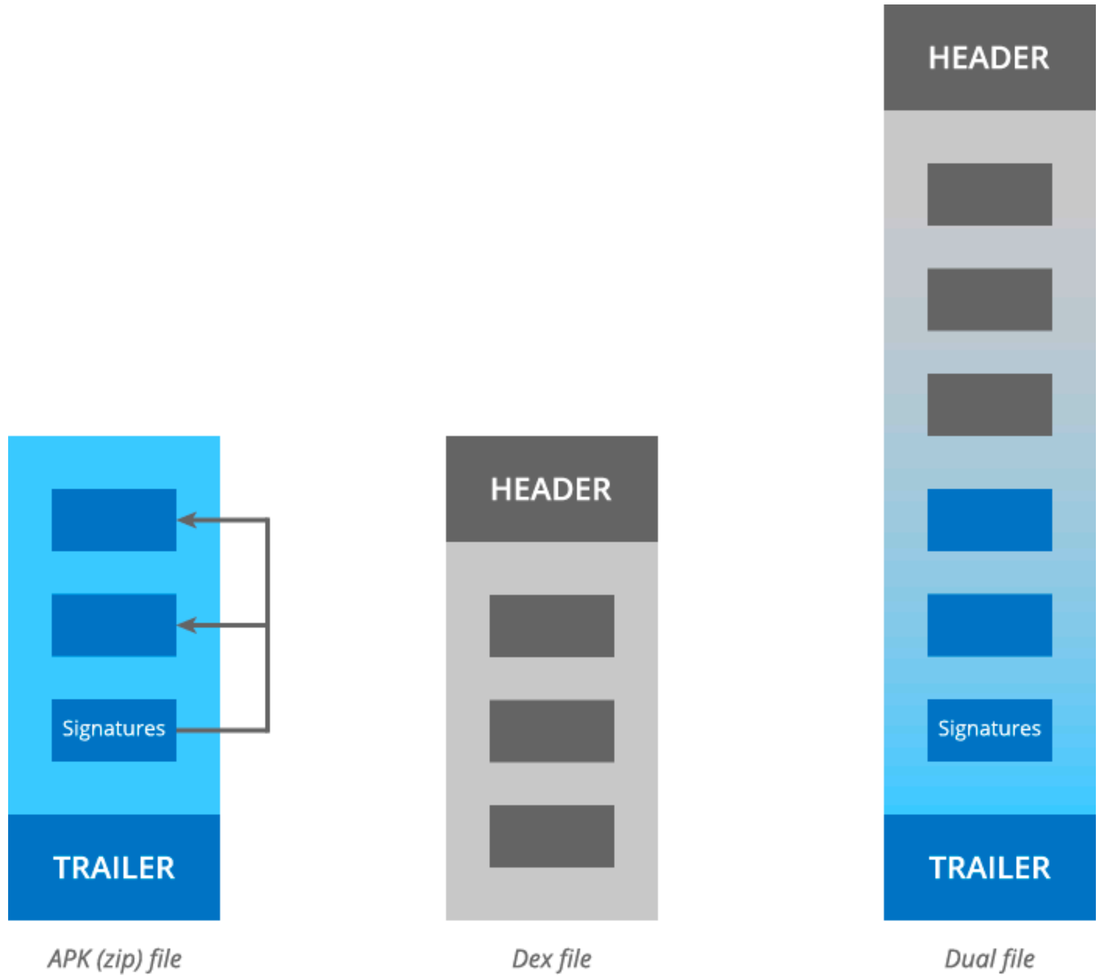
It's Slide 4 and I Haven't Even Told You What this Talk is About!

- Each issue of PoC||GTFO is a polyglot: a file that can be interpreted multiple ways depending on how it is parsed
- Usually crafted by **Ange Albertini**, **Philippe Teuwen**, myself, or some subset of the three of us
- This talk is about the ones I've contributed to
- **Goal**: Convince you that polyglots aren't just a nifty parlor trick

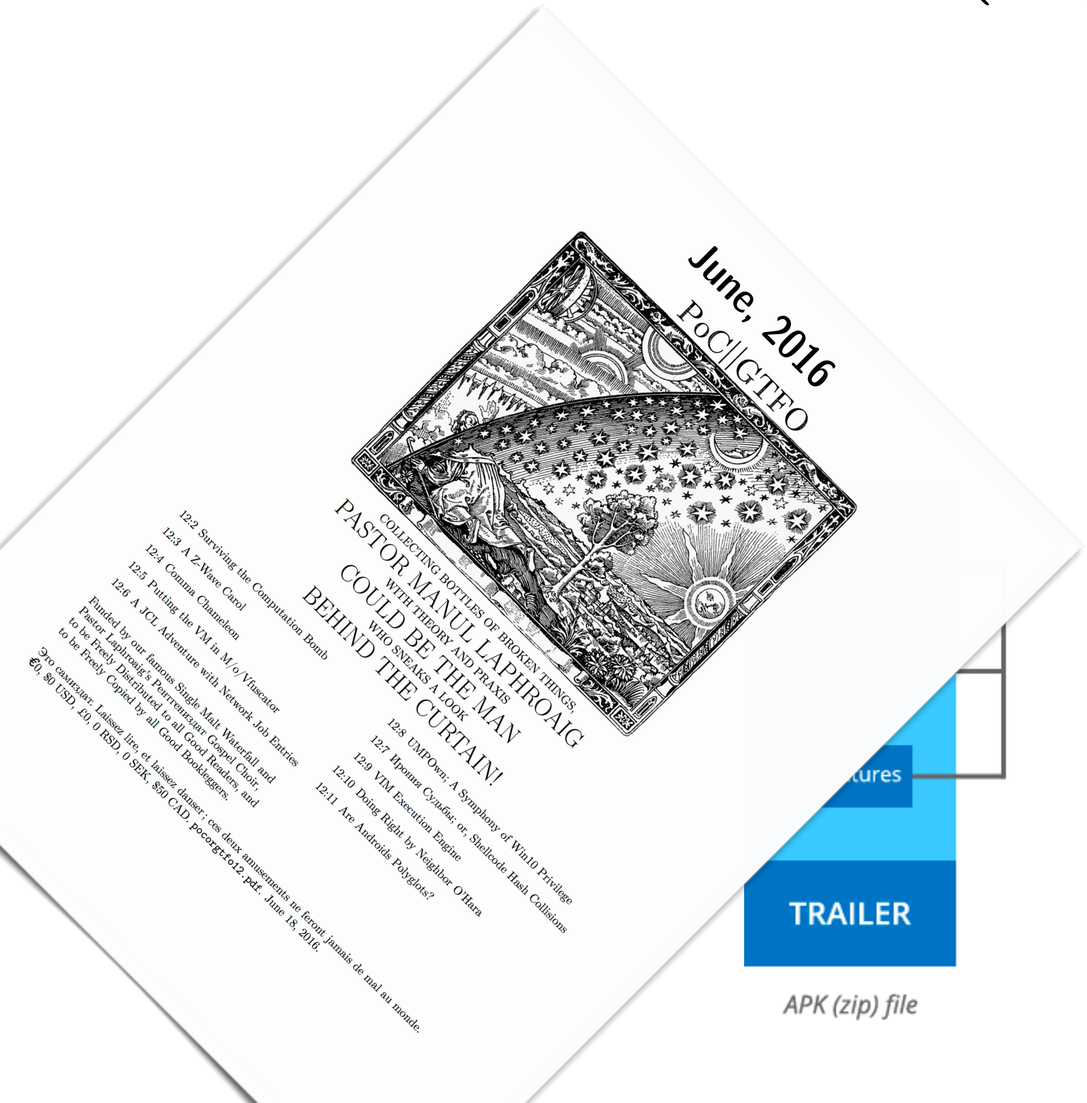
Man of The Book	Manul Laphroaig
Editor of Last Resort	Melilot
TEXnician	Evan Sultanik
Editorial Whipping Boy	Jacob Torrey
Funky File Supervisor	Ange Albertini
Assistant Scenic Designer	Philippe Teuwen
Scooby Crew Bus Driver	Ryan Speers

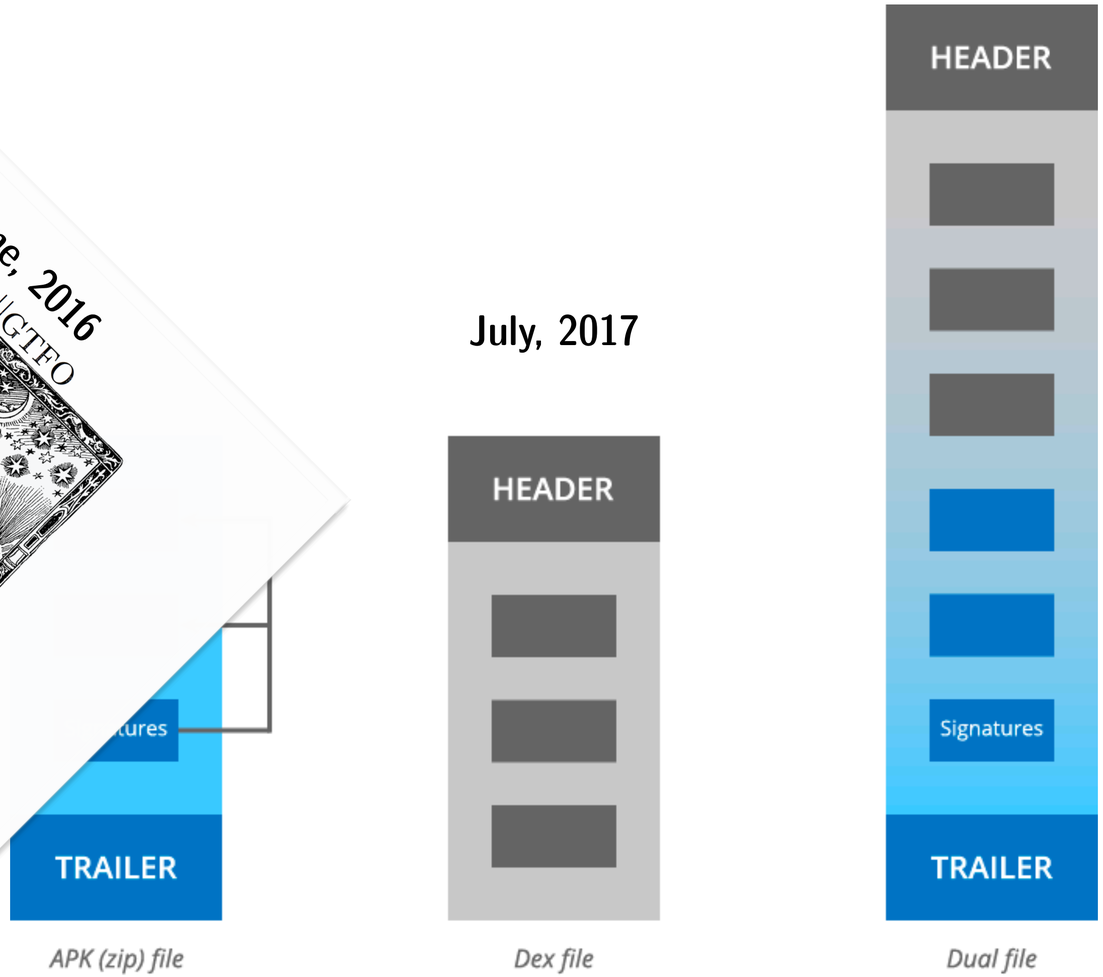
and sundry others

Example: Android APK (zip)/Dex Polyglot



Example: Android APK (zip)/Dex Polyglot





Before we get to more PoC||GTFO...

Time to drop some 0-day!

```
$ tar xvf totally_not_malware.tar.gz
```

Before we get to more PoC||GTFO...
Time to drop some 0-day!

```
$ tar xvf totally_not_malware.tar.gz
```

Note: We didn't provide the `z` option!

Modern versions of `tar` automagically detect that the archive is compressed based on magic bytes!
(The actual file extension is ignored.)

Before we get to more PoC||GTFO...
Time to drop some 0-day!

```
$ tar xvf totally_not_malware.tar.gz
```

Note: We didn't provide the `z` option!

Modern versions of `tar` automagically detect that the archive is compressed based on magic bytes!
(The actual file extension is ignored.)

🤔

What if we created a file that is *both* a valid `.tar` *and* a valid `.tar.gz`?

totally_not_malware.tar


DEFCON

Why are PDFs Particularly Polyglottable?

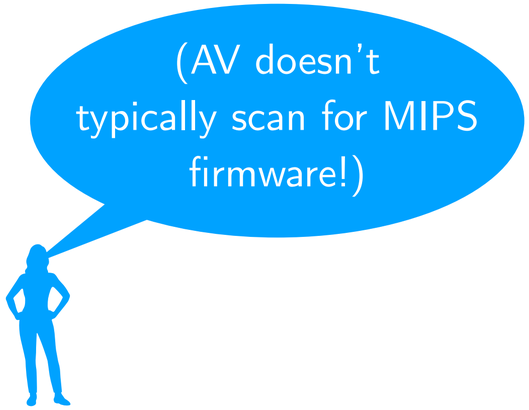
- Because "Adobe," that's why!
- It's been around for a long time
- Parsers built to be resilient to all sorts of errors and incompatibilities
- Can insert arbitrary length binary blobs almost anywhere in the file
- Almost all parsers ignore everything before the header

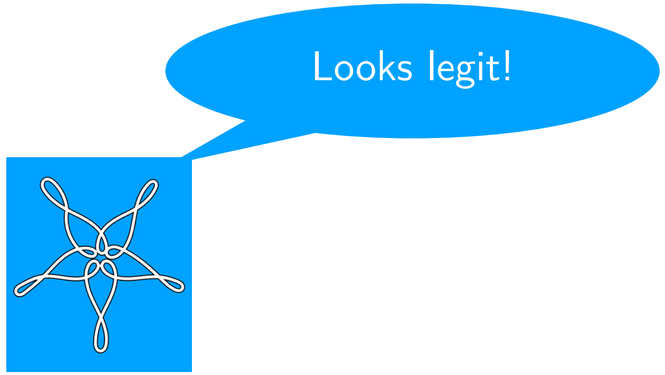
```
9999 0 obj
<<
/Length # bytes in the blob
>>
stream
lol, put whatever you want here!
endstream
endobj
```

```
lol, put whatever you want here!
%PDF-1.5
%<D0><D4><C5><D8>
        ⋮
```

Hey,
I've been trying to get my résumé to so-and-so in HR, but we've had problems with E-mail. Can you please print out the attached copy and give it to them?

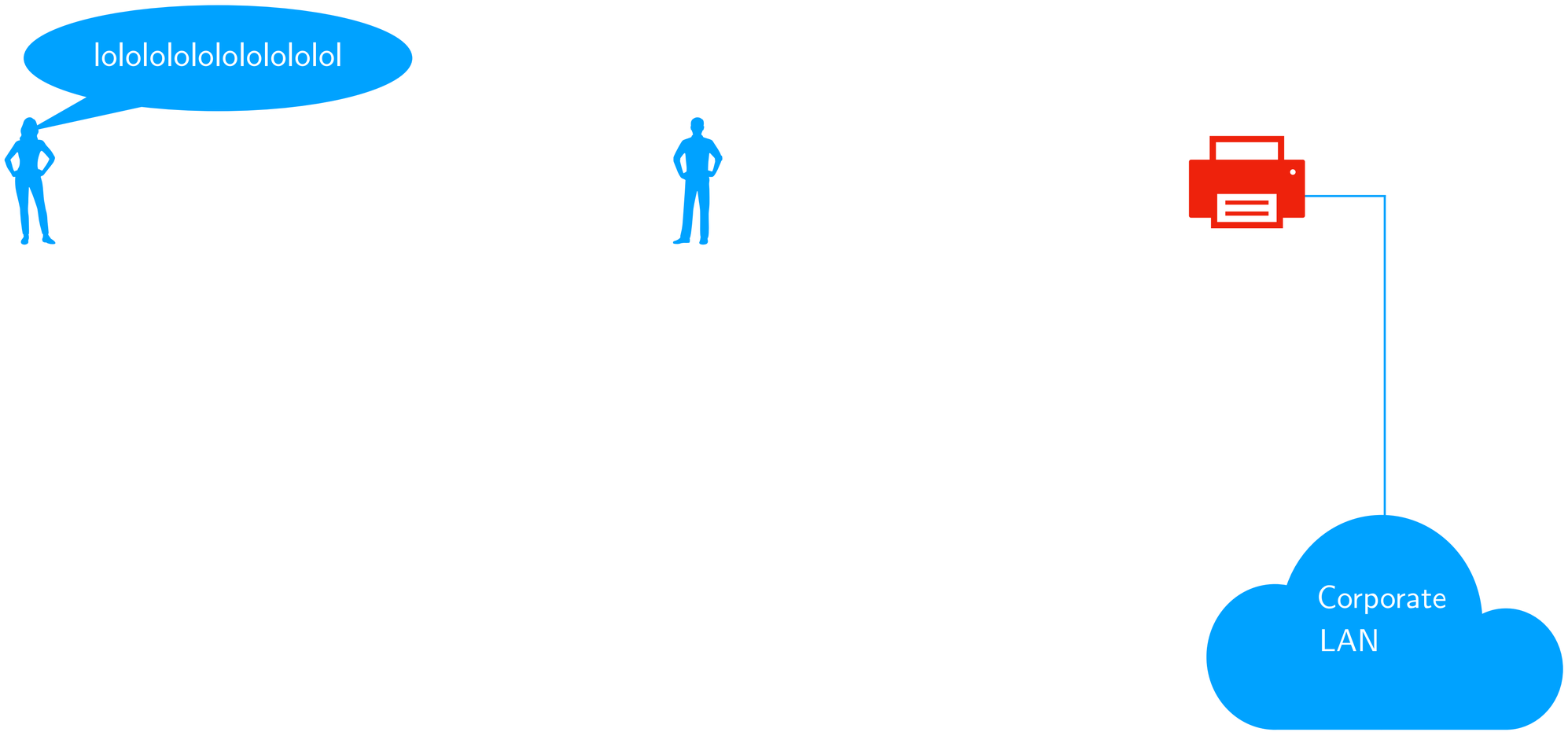
Thanks! —Alice Hackerman





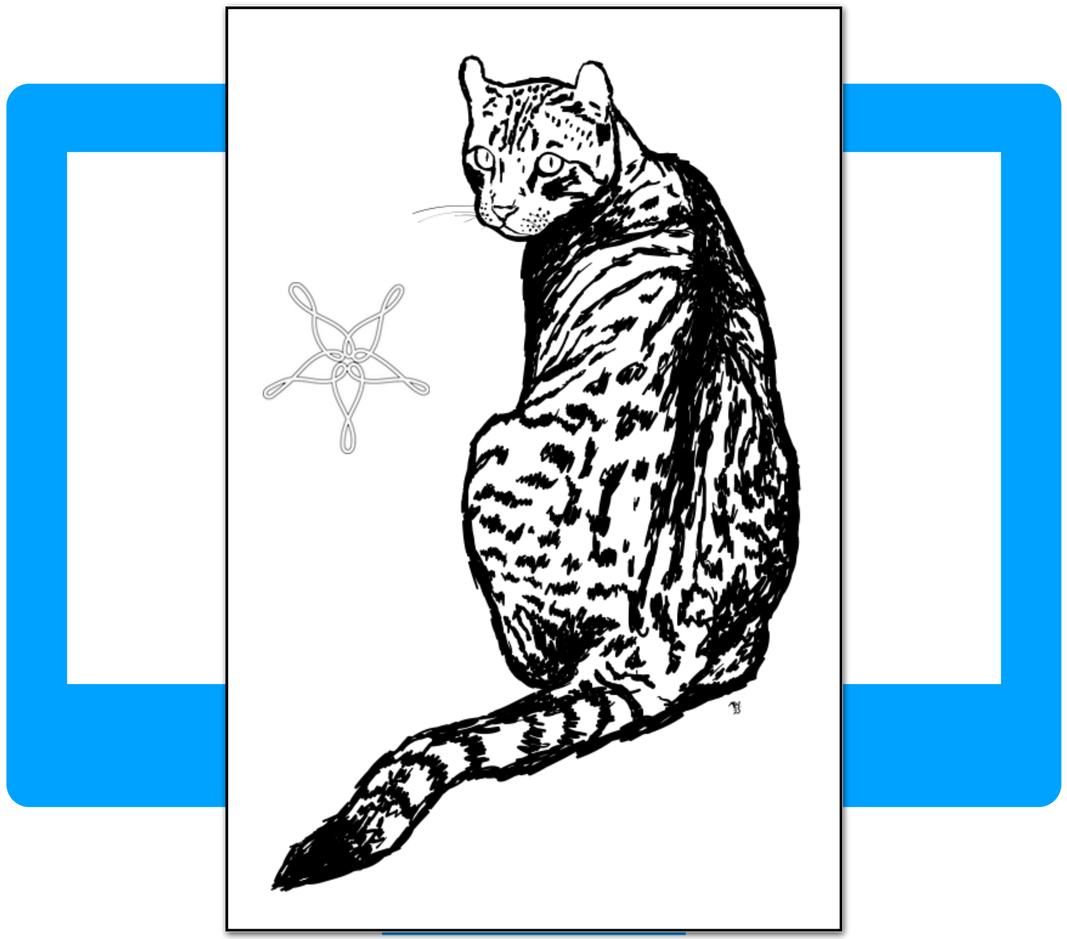
Hey,
I've been trying to get my résumé to so-and-so in HR, but we've had problems with E-mail. Can you please print out the attached copy and give it to them?

Thanks! —Alice Hackerman



PostScript/PJL (Cui & Stolfo, 2011)

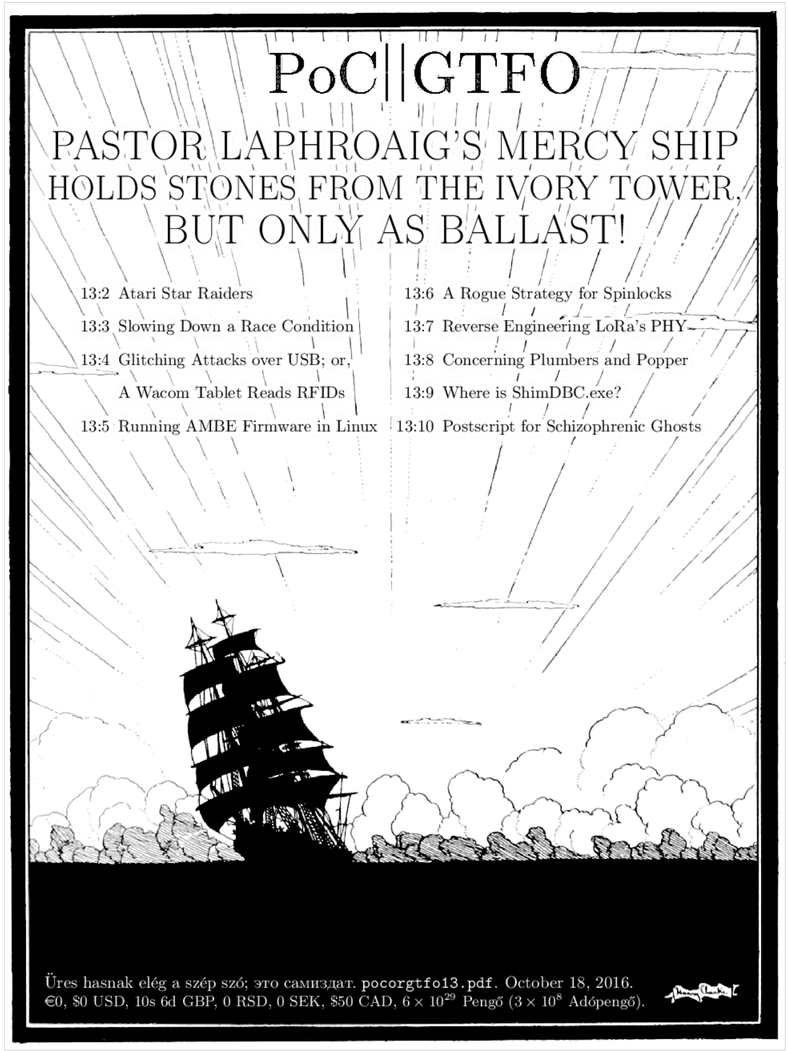
Producing a Positively Provocative PDF/PostScript Polyglot



Producing a Positively Provocative PDF/PostScript Polyglot

Don't print PostScript created by Weev!

PoC||GTFO 0x13



PoC||GTFO

PASTOR LAPHROAIG'S MERCY SHIP HOLDS STONES FROM THE IVORY TOWER, BUT ONLY AS BALLAST!

Üres hasnak elég a szép szó; это самиздат. pocorgtfo13.pdf. October 18, 2016.
€0, $0 USD, 10s 6d GBP, 0 RSD, 0 SEK, $50 CAD, 6×10^{29} Pengő (3×10^{8} Adópengő).

PDF

10 Post Scriptum: A Schizophrenic Ghost (Continued)

by Evan Sultanik and Philippe Teuwen

Once we got this PostScript polyglot working, the obvious next step was to decide what to put in it. We wanted to exhibit something you can't achieve in a PDF, so the following page contains an example that takes advantage of the fact that PostScript is a fully fledged Turing complete programming language. This feature of PostScript allows both *algorithmic compression* (*i.e.*, often a simple, short program can produce very complex output) and nondeterminism.

The following program is a quite amazing realization of David Bau from back in 1992, which will be regenerated every time you look at it. It is free puzzleware. Please distribute it and its output only for free, and keep his original comments intact. If you like it or if you have a suggestion, send him a postcard from your home town!

David Bau
777 South Avenue
Weston, MA 02193
USA
bau@cs.cornell.edu

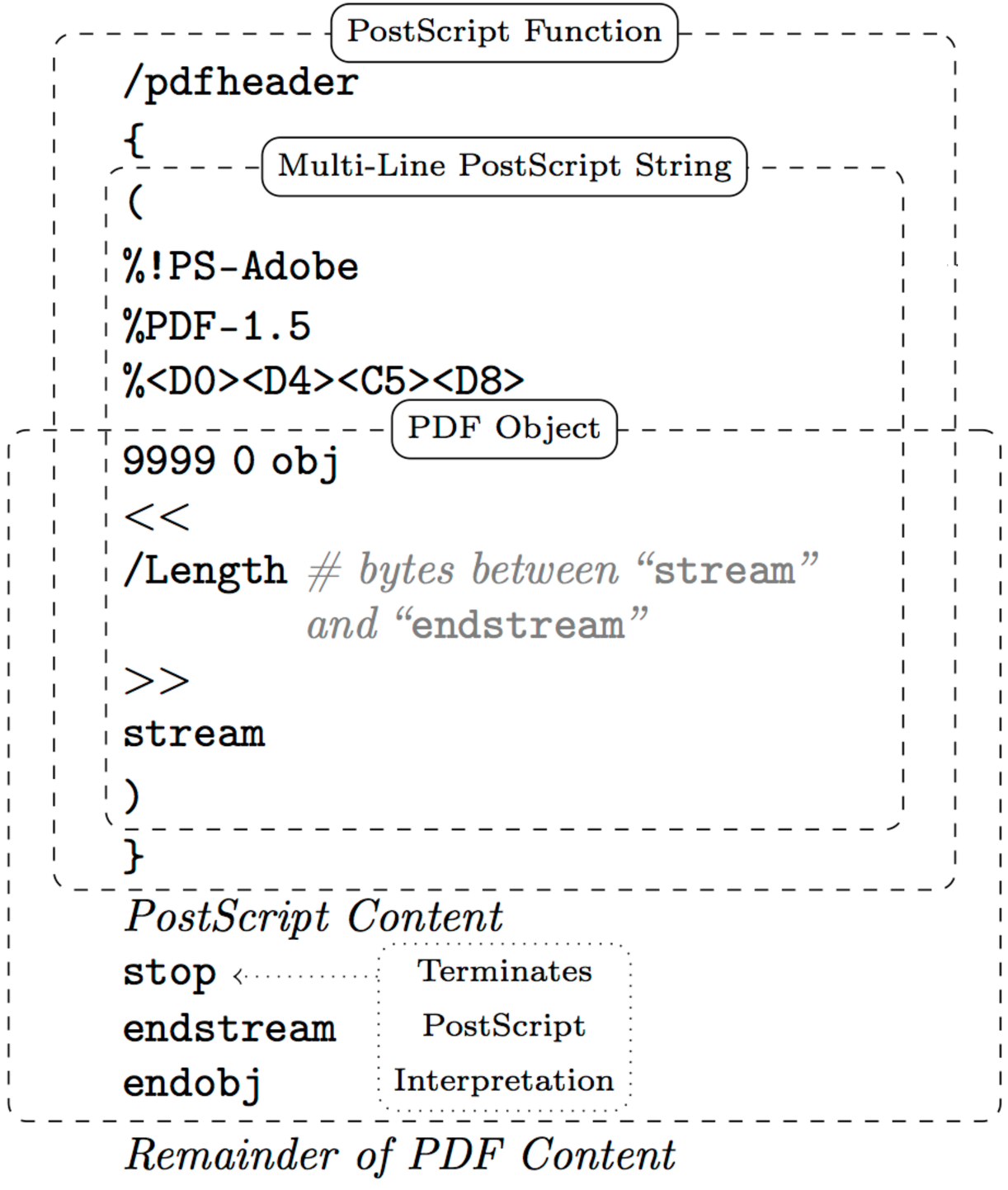
Don't be shy; hack the code! You can tune this puzzle into an easier one if you disable tunneling or downplay its twistiness...

Finally, remember to check out the page after the puzzle for a closing demonstration of PostScript's capabilities.

PostScript

- The PDF format is a *subset* of the PostScript language, meaning that we need to devise a way to get a PDF interpreter to ignore the PostScript code, and *vice versa*

- It's almost impossible to find a PostScript interpreter that doesn't *also* support PDF

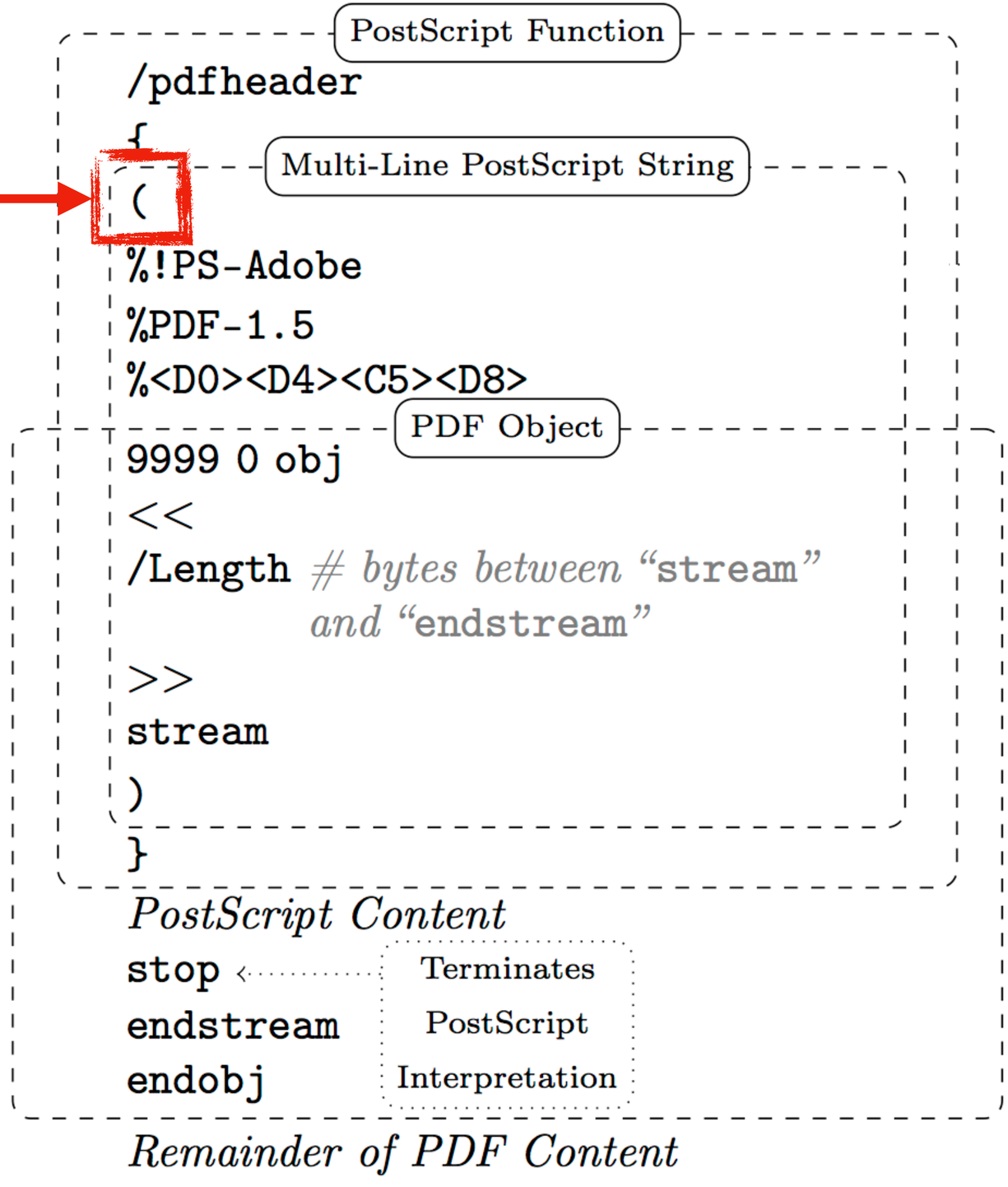


It would have been sufficient to just start the polyglot with an opening parenthesis, but we can't do that because Adobe has blacklisted all PDFs that start with a parenthesis.

Why? Because "Adobe," that's why!

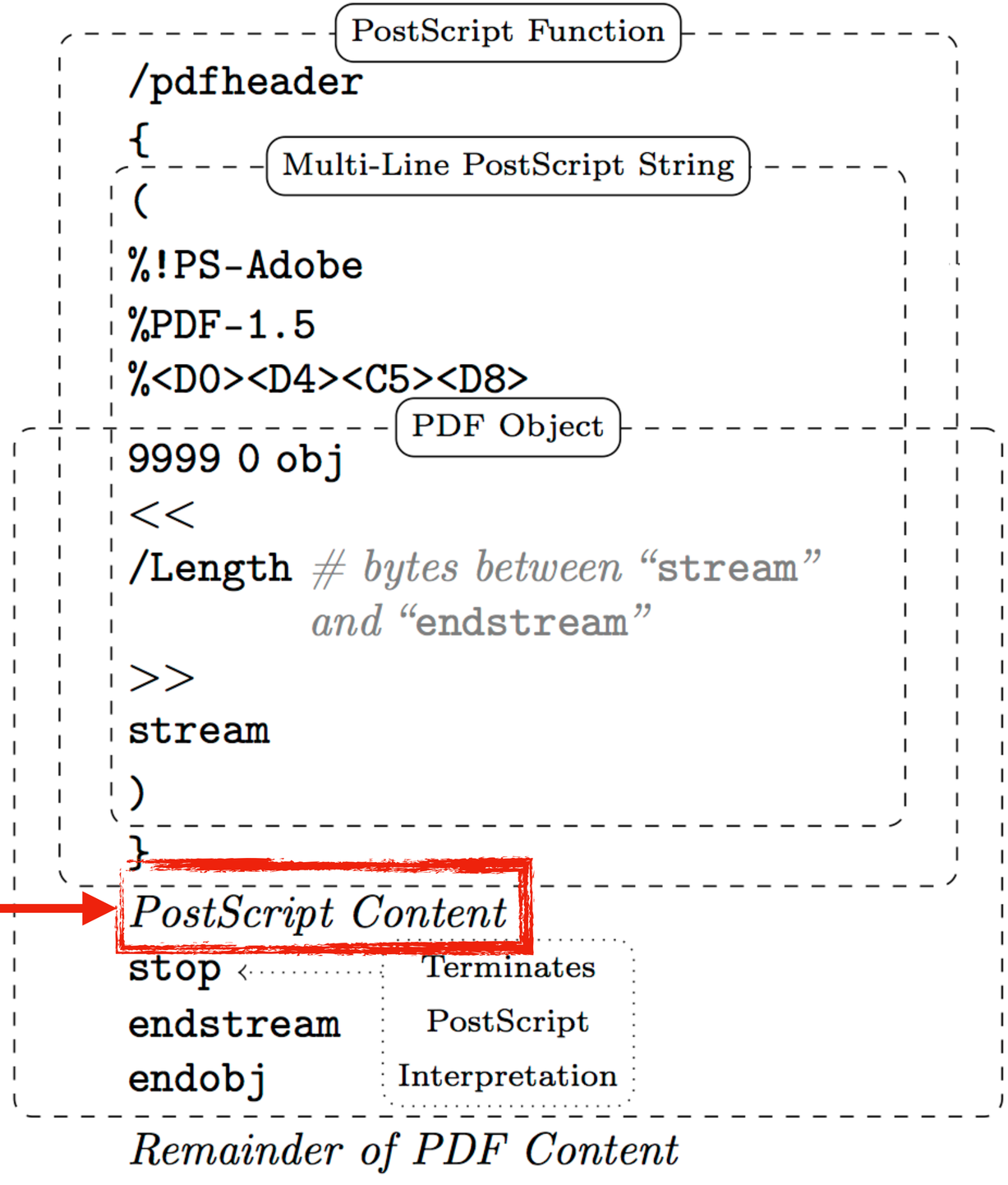
- The PDF format is a *subset* of the PostScript language, meaning that we need to devise a way to get a PDF interpreter to ignore the PostScript code, and *vice versa*

- It's almost impossible to find a PostScript interpreter that doesn't *also* support PDF



```
⋮
%%EndDocument
 @endspecial 0 TeXcolorgray 0 TeXcolorgray eop end
%%Trailer

userdict /end-hook known{end-hook}if
%%EOF

stop
```

How do we tell the PostScript interpreter to stop interpreting?



Ghostview /psi/dscparse.c

```
static int
dsc_scan_type(CDSC *dsc)
{
    unsigned char *p;
    unsigned char *line = (unsigned char *)(dsc->data + dsc->data_index);
    int length = dsc->data_length - dsc->data_index;

    /* Types that should be known:
     *   DSC
     *   EPSF
     *   PJL + any of above
     *   ^D + any of above
     *   DOS EPS
     *   PDF
     *   non-DSC
     */
```

Plus 164 more lines of complex logic!

Ghostview /psi/dscparse.c

```
static int
dsc_scan_type(CDSC *dsc)
{
    unsigned char *p;
    unsigned char *line = (unsigned char *)(dsc->data + dsc
    int length = dsc->data_length - dsc->data_index;

    /* Types that should be known:
     *   DSC
     *   EPSF
     *   PJL + any of above
     *   ^D + any of above
     *   DOS EPS
     *   PDF
     *   non-DSC
     */
```

Plus 164 more lines of complex logic!

```
if (COMPARE(dsc->line, "%!PS-Adobe")) {
    dsc->dsc = TRUE;
    dsc->begincomments = DSC_START(dsc);
    if (dsc->dsc_version == NULL)
        return CDSC_ERROR;  /* no memory */
    p = (unsigned char *)dsc->line + 14;
    while (IS_WHITE(*p))
        p++;
    if (COMPARE(p, "EPSF-"))
        dsc->epsf = TRUE;
    dsc->scan_section = scan_comments;
    return CDSC_PSADOBE;
}
if (COMPARE(dsc->line, "%!")) {
    dsc->scan_section = scan_comments;
    return CDSC_NOTDSC;
}
```

Ghostview /psi/dscparse.c

```
static int
dsc_scan_type(CDSC *dsc)
{
    unsigned char *p;
    unsigned char *line = (unsigned char *)(dsc->data + dsc
    int length = dsc->data_length - dsc->data_index;

    /* Types that should be known:
     *   DSC
     *   EPSF
     *   PJL + any of above
     *   ^D + any of above
     *   DOS EPS
     *   PDF
     *   non-DSC
     */
```

Plus 164 more lines of complex logic!

```
if (COMPARE(dsc->line, "%!PS-Adobe")) {
    dsc->dsc = TRUE;
    dsc->begincomments = DSC_START(dsc);
    if (dsc->dsc_version == NULL)
        return CDSC_ERROR;  /* no memory */
    p = (unsigned char *)dsc->line + 14;
    while (IS_WHITE(*p))
        p++;
    if (COMPARE(p, "EPSF-"))
        dsc->epsf = TRUE;
    dsc->scan_section = scan_comments;
    return CDSC_PSADOBE;
}
if (COMPARE(dsc->line, "%!")) {
    dsc->scan_section = scan_comments;
    return CDSC_NOTDSC;
}
```

Interpret the file as PostScript

Interpret the file as a PDF

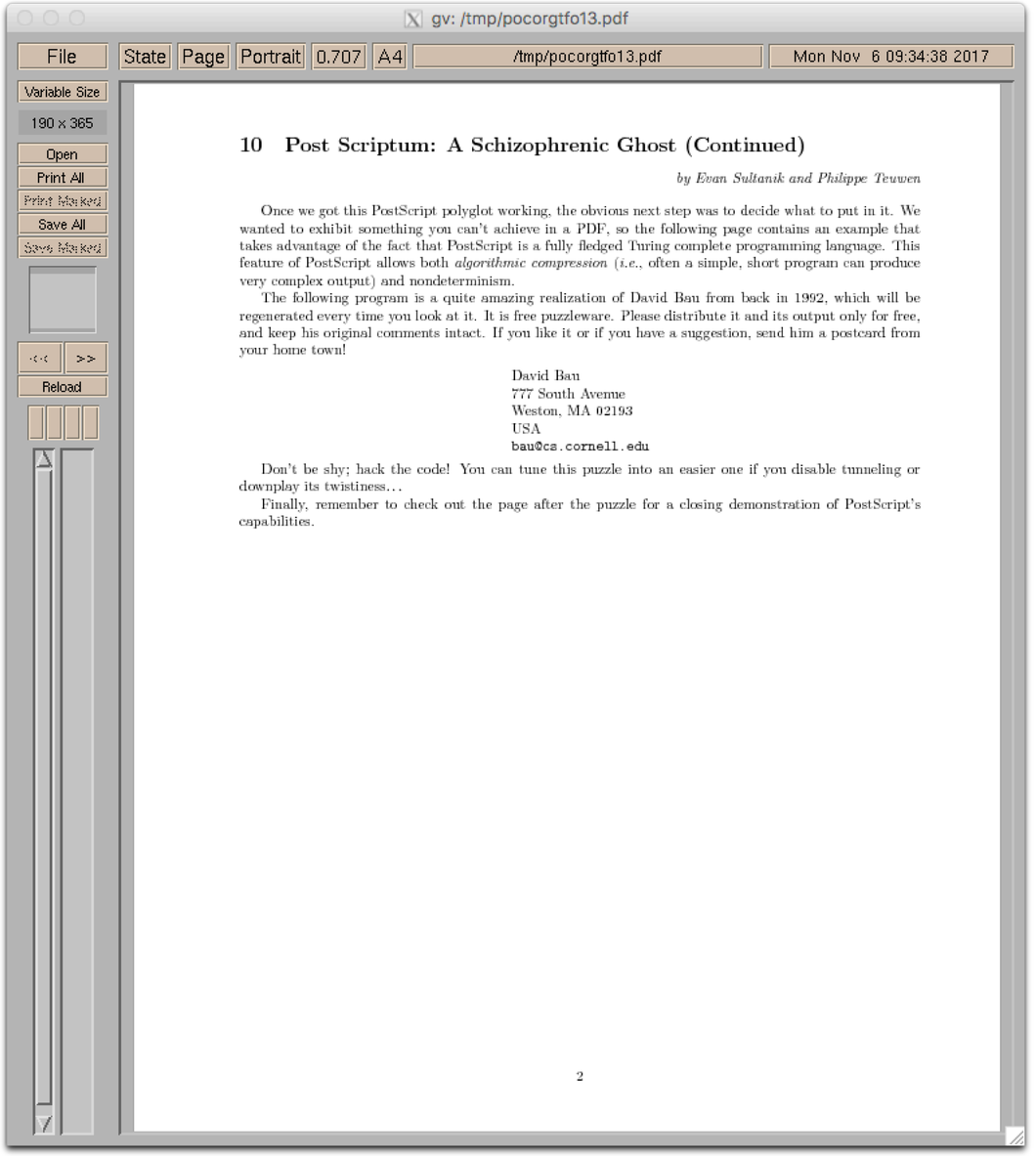
Ghostview /psi/dscparse.c

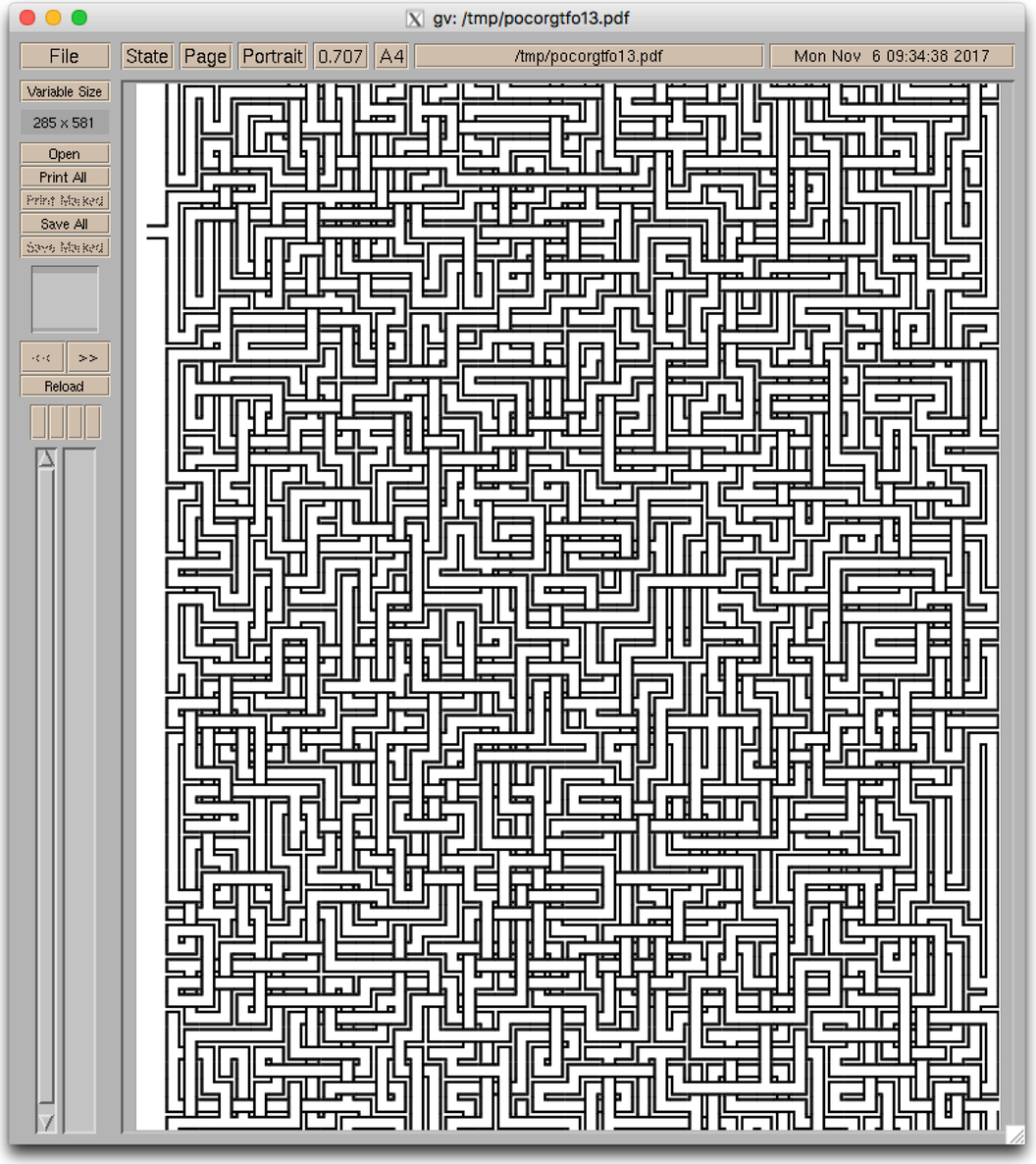
```
static int
dsc_scan_type(CDSC *dsc)
{
    unsigned char *p;
    unsigned char *line = (unsigned char *)dsc->line + dsc->data_index;
    int length = dsc->data_length - dsc->data_index;

    /* Types that should be known:
     *   DSC
     *   EPSF
     *   PJL + any of above
     *   ^D + any of above
     *   DOS EPS
     *   PDF
     *   non-DSC
     */
```

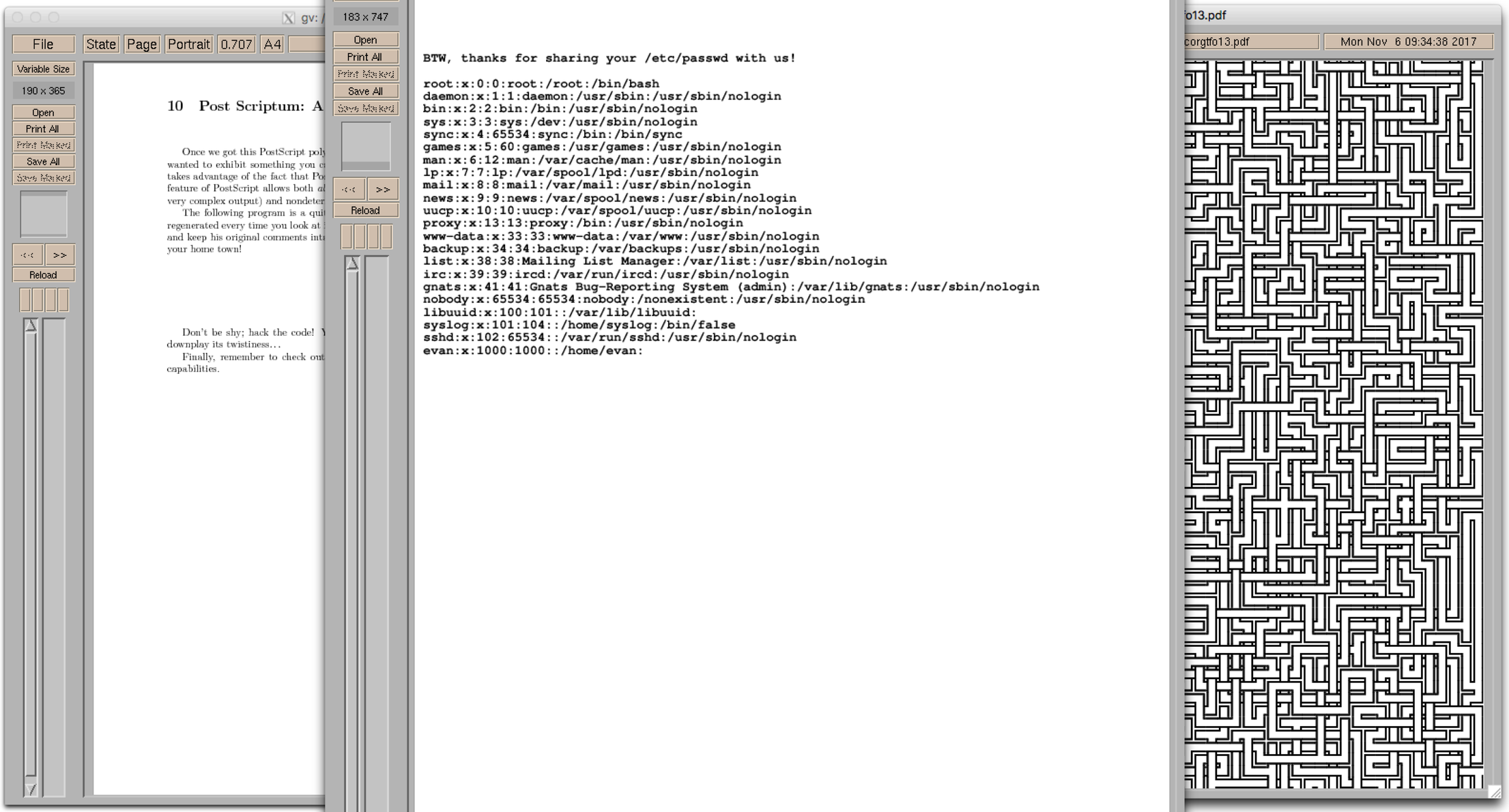
```
    if (COMPARE(dsc->line, "%!PS-Adobe")) {
        dsc->dsc = TRUE;
        dsc->begincomments = DSC_START(dsc);
        if (dsc->dsc_version == NULL)
            return CDSC_ERROR;  /* no memory */
        p = (unsigned char *)dsc->line + 14;
        while (IS_WHITE(*p))
            p++;
        if (COMPARE(p, "EPSF-"))
            dsc->epsf = TRUE;
        dsc->scan_section = sca
        Plus 164 more lines of complex lo
        return CDSC_PSADOBE;
    }
    if (COMPARE(dsc->line, "%!"
        dsc->scan_section = scan_comments;
        return CDSC_NOTDSC;
    }
```

%!PS-Adobe ← *this must come before*

%PDF-1.5 ← *this*

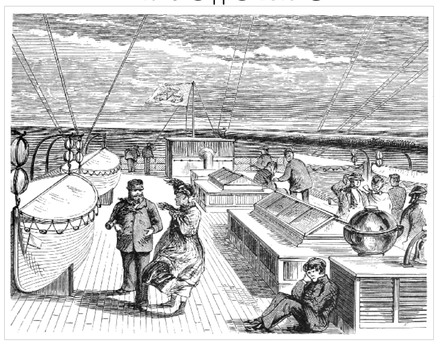

gv: /tmp/pocorgtfo13.pdf
File
State
Page
Portrait
0.707
A4
/tmp/pocorgtfo13.pdf
Mon Nov 6 09:34:38 2017
Variable Size
190 x 365
Open
Print All
Print Marked
Save All
Save Marked
<<
>>
Reload
10 Post Scriptum: A Schizophrenic Ghost (Continued)
by Evan Sultanik and Philippe Teuwen
Once we got this PostScript polyglot working, the obvious next step was to decide what to put in it. We wanted to exhibit something you can't achieve in a PDF, so the following page contains an example that takes advantage of the fact that PostScript is a fully fledged Turing complete programming language. This feature of PostScript allows both algorithmic compression (i.e., often a simple, short program can produce very complex output) and nondeterminism.
The following program is a quite amazing realization of David Bau from back in 1992, which will be regenerated every time you look at it. It is free puzzleware. Please distribute it and its output only for free, and keep his original comments intact. If you like it or if you have a suggestion, send him a postcard from your home town!
David Bau
777 South Avenue
Weston, MA 02193
USA
bau@cs.cornell.edu
Don't be shy; hack the code! You can tune this puzzle into an easier one if you disable tunneling or downplay its twistiness...
Finally, remember to check out the page after the puzzle for a closing demonstration of PostScript's capabilities.
2


gv: /tmp/pocorgtfo13.pdf
File
State
Page
Portrait
0.707
A4
/tmp/pocorgtfo13.pdf
Mon Nov 6 09:34:38 2017
Variable Size
285 x 581
Open
Print All
Print Marked
Save All
Save Marked
<<
>>
Reload


gv: /tmp/pocorgtfo13.pdf
File
State
Page
Portrait
1.000
A4
/tmp/pocorgtfo13.pdf
Sat Oct 22 08:37:57 2016
Variable Size
183 x 747
Open
Print All
Print Marked
Save All
Save Marked
<<
>>
Reload
BTW, thanks for sharing your /etc/passwd with us!
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
evan:x:1000:1000::/home/evan:
File
State
Page
Portrait
0.707
A4
Variable Size
190 x 365
Open
Print All
Print Marked
Save All
Save Marked
<<
>>
Reload
10 Post Scriptum: A
Once we got this PostScript poly
wanted to exhibit something you c
takes advantage of the fact that Po
feature of PostScript allows both al
very complex output) and nondeter
The following program is a qui
regenerated every time you look at
and keep his original comments int
your home town!
Don't be shy; hack the code! Y
downplay its twistiness...
Finally, remember to check out
capabilities.
Mon Nov 6 09:34:38 2017

HTTP Quine

PoC||GTFO



IN A FIT OF STUBBORN OPTIMISM,

PASTOR MANUL LAPHROAIG

AND HIS CLEVER CREW

SET SAIL TOWARD

WELCOMING SHORES OF

THE GREAT UNKNOWN!

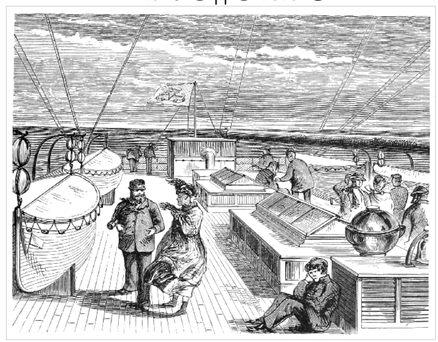
Heidelberg, Baden-Württemberg

Funded by our famous Single Malt Waterfall and Pastor Laphroaig's Рентгеновидат Gospel Choir, to be Freely Distributed to all Good Readers, and to be Freely Copied by all Good Bookleggers.

Это самиздат. Denn was man Schwarz auf Weiß besitzt, kann man getrost nach Hause tragen. €0, $0 USD, £0, 0 RSD, 0 SEK, $50 CAD. `pocorgtfo11.pdf`. March 17, 2016.

HTTP Quine

PoC||GTFO



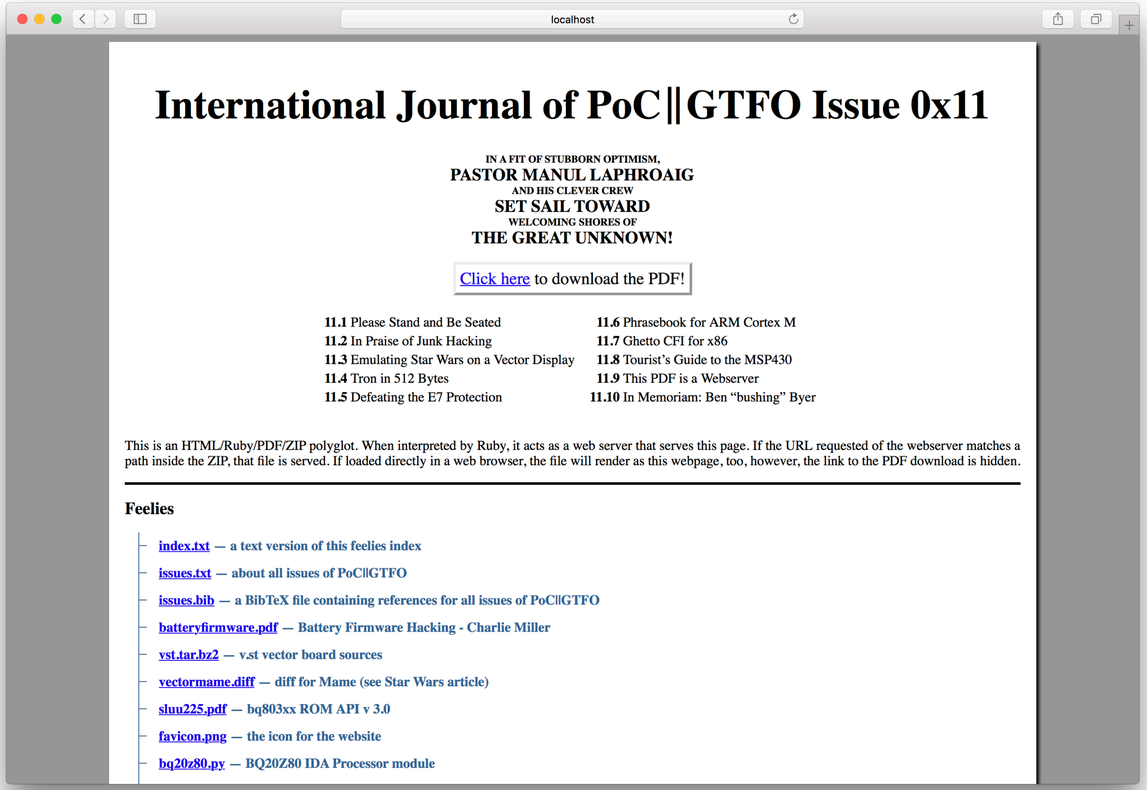
IN A FIT OF STUBBORN OPTIMISM,
PASTOR MANUL LAPHROAIG
AND HIS CLEVER CREW
SET SAIL TOWARD
WELCOMING SHORES OF
THE GREAT UNKNOWN!

Heidelberg, Baden-Württemberg

Funded by our famous Single Malt Waterfall and Pastor Laphroaig's Рентгениздат Gospel Choir, to be Freely Distributed to all Good Readers, and to be Freely Copied by all Good Bookleggers.

Это самиздат. Denn was man Schwarz auf Weiß besitzt, kann man getrost nach Hause tragen.
€0, $0 USD, £0, 0 RSD, 0 SEK, $50 CAD. `pocorgtfo11.pdf`. March 17, 2016.


```
$ ruby pocorgtfo11.pdf
Listening for connections on port 8080.
To listen on a different port,
re-run with the desired port as a command-line argument.
```



HTTP Quine

PA

11:1 Please Stand and Be
11:2 In Praise of Junk Ha
11:3 Emulating Star War
11:4 Tron in 512 Bytes
11:5 Defeating the E7 Pro

Heidelberg, Baden-Württe

Funded by our famous Sin
Pastor Laphroaig's Pennre
to be Freely Distributed t
to be Freely Copied by all

Это самиздат. Denn was
€0, $0 USD, £0, 0 RSD,

argument.

localhost

International Journal of PoC||GTFO Issue 0x11

IN A FIT OF STUBBORN OPTIMISM,
PASTOR MANUL LAPHROAIG
AND HIS CLEVER CREW
SET SAIL TOWARD
WELCOMING SHORES OF
THE GREAT UNKNOWN!

Click here to download the PDF!

This is an HTML/Ruby/PDF/ZIP polyglot. When interpreted by Ruby, it acts as a web server that serves this page. If the URL requested of the webserver matches a path inside the ZIP, that file is served. If loaded directly in a web browser, the file will render as this webpage, too, however, the link to the PDF download is hidden.

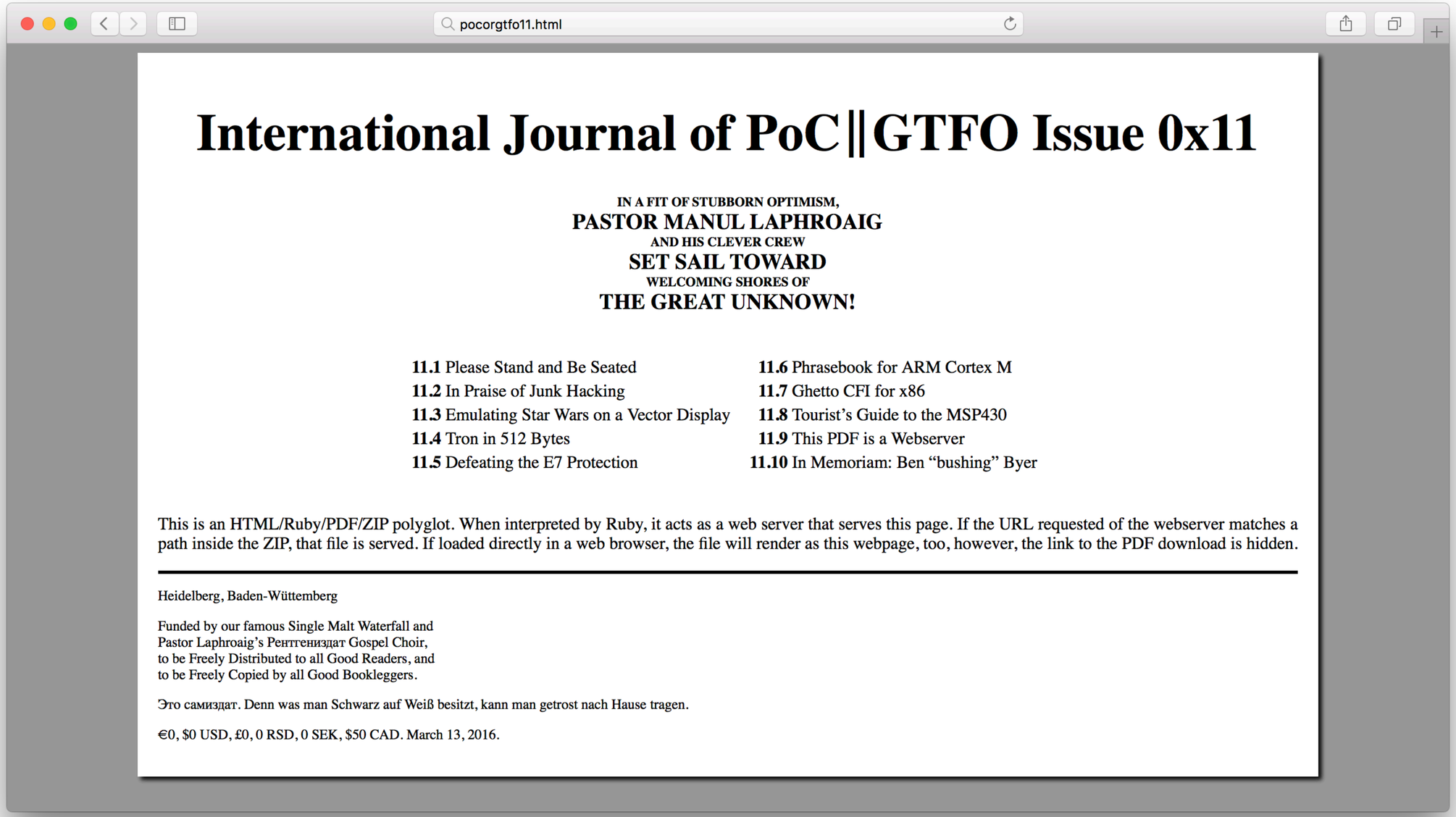
Feelies

- **index.txt — a text version of this feelies index**
- **issues.txt — about all issues of PoC||GTFO**
- **issues.bib — a BibTeX file containing references for all issues of PoC||GTFO**
- **batteryfirmware.pdf — Battery Firmware Hacking - Charlie Miller**
- **vst.tar.bz2 — v.st vector board sources**
- **vectormame.diff — diff for Mame (see Star Wars article)**
- **sluu225.pdf — bq803xx ROM API v 3.0**
- **favicon.png — the icon for the website**
- **bq20z80.py — BQ20Z80 IDA Processor module**

But Wait, There's More!

```
$ ln -s pocorgtfo11.pdf pocorgtfo11.html
```

But Wait, There's More!



International Journal of PoC||GTFO Issue 0x11

IN A FIT OF STUBBORN OPTIMISM,
PASTOR MANUL LAPHROAIG
AND HIS CLEVER CREW
SET SAIL TOWARD
WELCOMING SHORES OF
THE GREAT UNKNOWN!

This is an HTML/Ruby/PDF/ZIP polyglot. When interpreted by Ruby, it acts as a web server that serves this page. If the URL requested of the webserver matches a path inside the ZIP, that file is served. If loaded directly in a web browser, the file will render as this webpage, too, however, the link to the PDF download is hidden.

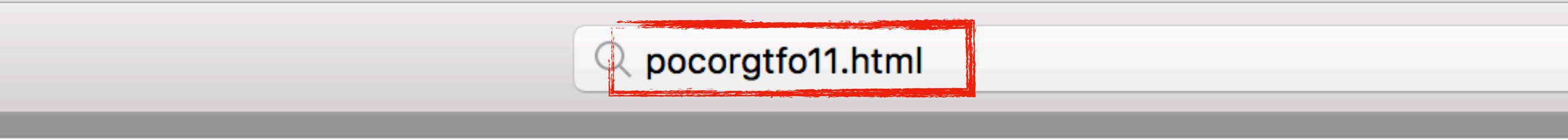
Heidelberg, Baden-Württemberg

Funded by our famous Single Malt Waterfall and
Pastor Laphroaig's Рентгениздат Gospel Choir,
to be Freely Distributed to all Good Readers, and
to be Freely Copied by all Good Bookleggers.

Это самиздат. Denn was man Schwarz auf Weiß besitzt, kann man getrost nach Hause tragen.

€0, $0 USD, £0, 0 RSD, 0 SEK, $50 CAD. March 13, 2016.

But Wait, There's More!



nternational Journal of Po

IN A FIT OF STUBBORN OPTI

PASTOR MANUL LAPI

In which an HTML page is also a PDF

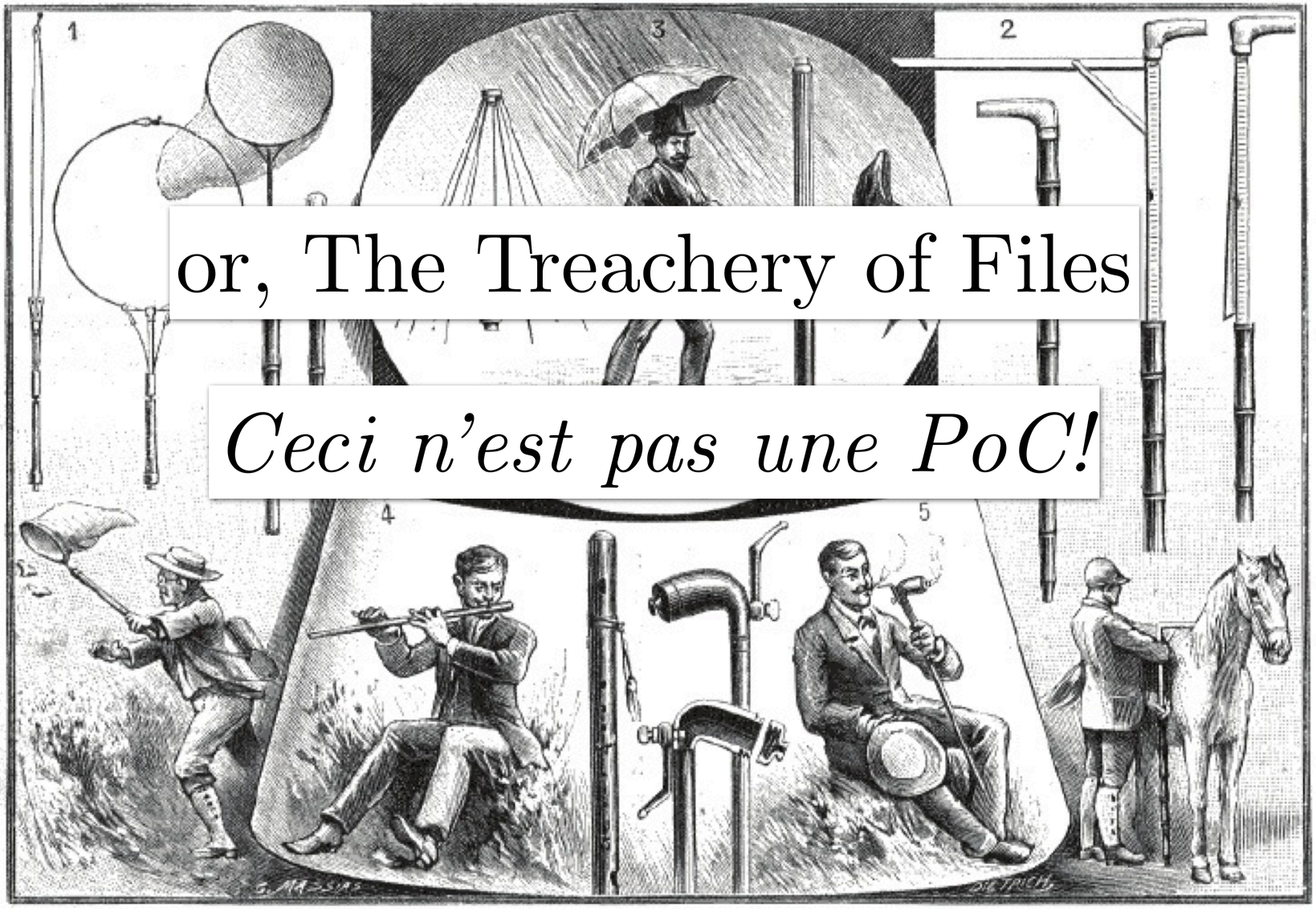
Which is also a ZIP

Which is also a Ruby script

Which is an HTTP Quine

or, The Treachery of Files

Ceci n'est pas une PoC!



Utilisation de la canne. — 1. Canne-filet à papillons. — 2. Canne à toiser les chevaux. — 3. Canne-parapluie. — 4. Canne musicale. — 5. Ceci n'est pas une pipe.

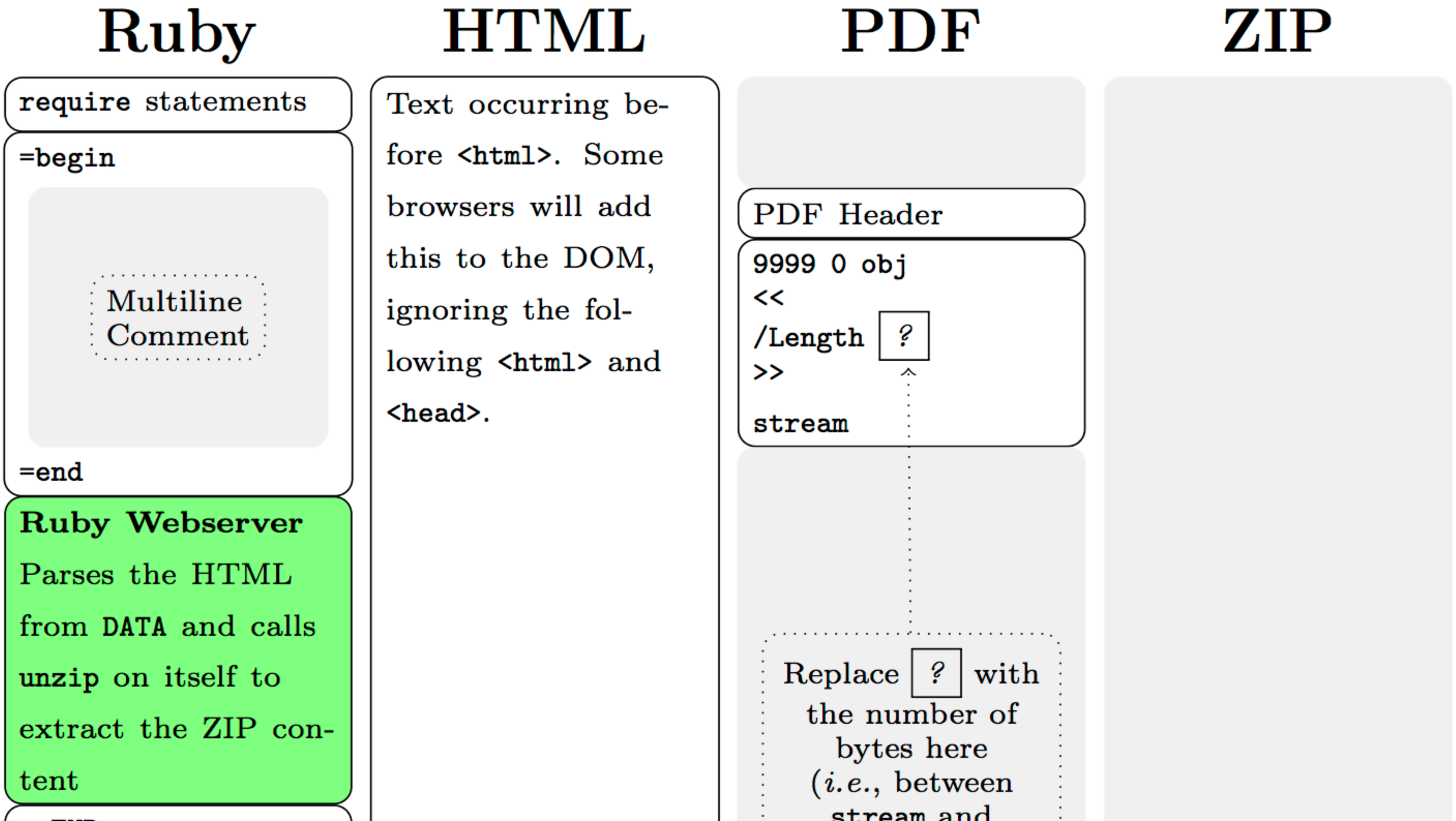
Minimal PoC

Simply prepend this to any PDF!

```
require 'socket'
server = TCPServer.new('', 8080) loop do
socket = server . accept
request = socket . gets
response = File.open(__FILE__).read socket . print "HTTP/1.1 200 OK\r\n" +
"Content-Type: application/pdf\r\n" +
"Content-Length : #{response . bytesize}\r\n" +
"Connection: close\r\n" socket . print "\r\n"
socket . print response socket . close
end
__END__
```

But why stop there?

```
require 'socket'
server = TCPServer.new('', 8080)
html = DATA.read().split(/<\/html>/)[0]+"</html>\n"
loop do
        socket = server.accept
        if socket.gets.split(' ')[1].downcase.end_with? ".pdf" then
            c = "application/pdf"
            d = File.open(__FILE__).read
            n = File.size(__FILE__)
        else
            c = "text/html"
            d = html
            n = html.length
        end
        socket.print "HTTP/1.1 200 OK\r\nContent-Type: #{c}\r\nContent-Length: #{n}\r\nConnection: close\r\n\r\n"+d
        socket.close
end
__END__
<html>
  <head>
    <title>An HTTP Quine PoC</title>
  </head>
  <body>
    <a href="pocorgtfo11.pdf">Download pocorgtfo11.pdf!</a>
  </body>
</html>
```


Ruby
HTML
PDF
ZIP
require statements
=begin
Multiline Comment
=end
Ruby Webserver
Parses the HTML from DATA and calls unzip on itself to extract the ZIP content
Text occurring before <html>. Some browsers will add this to the DOM, ignoring the following <html> and <head>.
PDF Header
9999 0 obj
<<
/Length ?
>>
stream
Replace ? with the number of bytes here (i.e., between stream and

Ruby Webserver

Parses the HTML from `DATA` and calls `unzip` on itself to extract the ZIP content

`__END__`

Everything after `__END__` is accessible from Ruby's special `DATA` object

HTML

Javascript to remove everything between "require..." and "`__END__`" from the DOM, if necessary

`<!--`

Replace `?` with the number of bytes here (*i.e.*, between `stream` and `endstream`)

`endstream`

__END__
from the DOM, if necessary

<!--

endstream

endobj

PDF Content

obj/stream

ZIP Content
as usual
(cf. PoC||GTFO 1:5 and 9:12)

Central Directory

Archive Comment

endstream/endobj

PDF Footer

-->

PDF/NES Polyglot and MD5 Quine

PDF/NES Polyglot and MD5 Quine

```
char md5_part1[33];
char md5_part2[33];

unsigned char read_md5_byte(unsigned char byte) {
    static unsigned char bit;
    static uintptr_t offset;
    static unsigned char ret;
    ret = 0;
    for(bit=0; bit<8; ++bit) {
        ret <<= 1;
        offset = MD5_OFFSET + 128 * 8 * (uintptr_t)byte +
128*(uintptr_t)bit + MEMORY(MD5_DIFFS_OFFSET + 2 * 8 *
byte + 2 * bit);
        if(MEMORY(offset) == MEMORY(MD5_DI
* 8 * byte + 2 * bit + 1)) {
            ret |= 1;
        }
    }
    return ret;
}

char nibble_to_char(unsigned char nibble)
    if(nibble < 10) {
        return '0' + nibble;
    } else {
        return 'A' + nibble - 10;
    }
}

void read_md5() {
    static unsigned char i;
    for(i=0; i<8; ++i) {
        unsigned char byte = read_md5_byte
        md5_part1[i*3] = nibble_to_char(by
        md5_part1[i*3+1] = nibble_to_char(
        md5_part1[i*3+2] = ' ';
    }
    md5_part1[32] = '\0';
    for(i=0; i<8; ++i) {
        unsigned char byte = read_md5_byte
        md5_part2[i*3] = nibble_to_char(by
        md5_part2[i*3+1] = nibble_to_char(
        md5_part2[i*3+2] = ' ';
    }
    md5_part2[32] = '\0';
}
```

PoC||GTFO

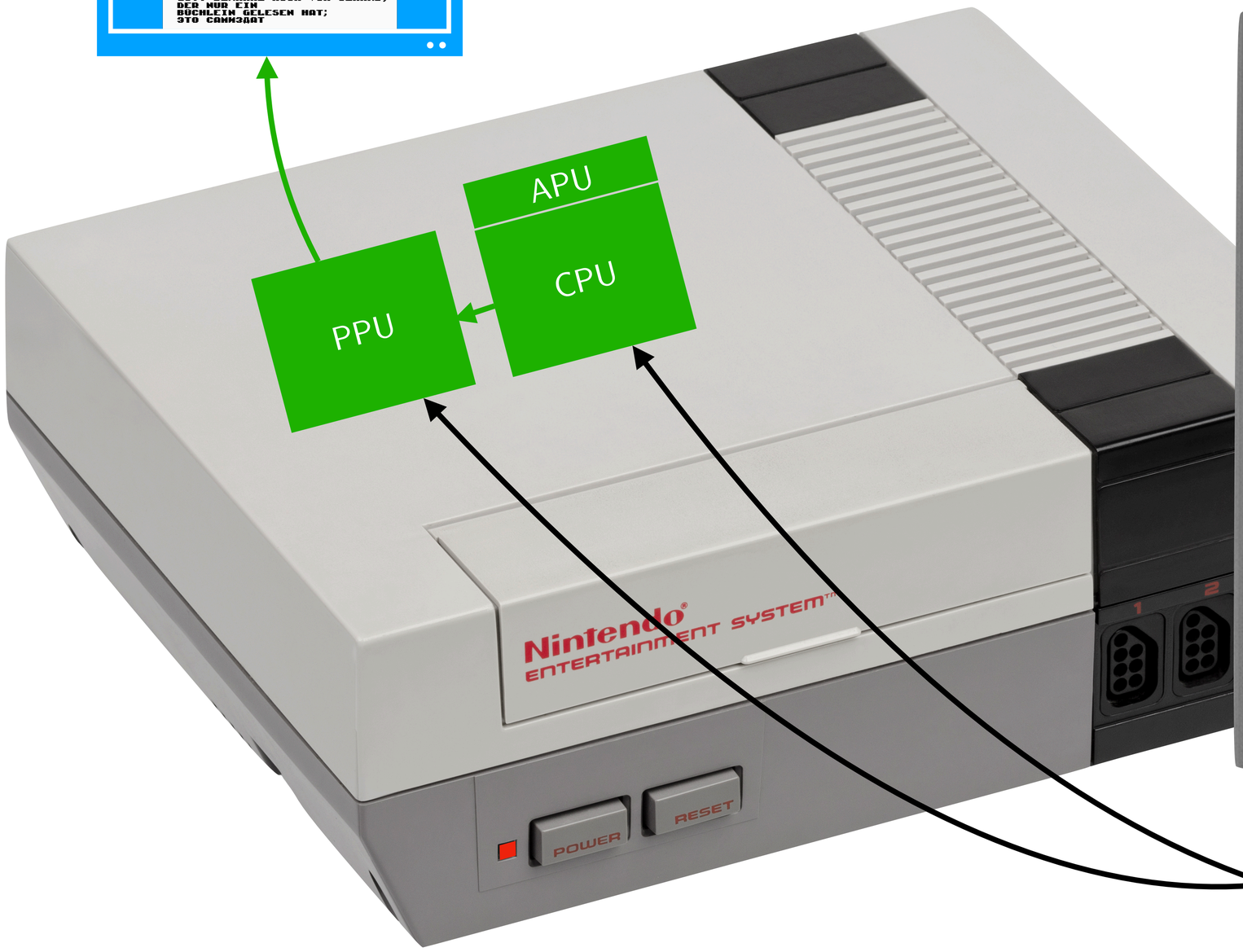
PASTOR LAPHROAIG SCREAMS
HIGH FIVE TO THE HEAVENS
AS THE WHOLE WORLD GOES UNDER

14:02 Z-Ring Phreaking
14:03 Concerning Desert Studies
14:04 Flush+Reload Side-Channel Attacks
14:05 Anti-Keylogging with Random Noise
14:06 Random NOPs on ARM
14:07 Ethernet Over GDB
14:08 Control Panel Vulnerabilities
14:09 MD5 Postscript
14:10 MD5 PDF
14:11 MD5 GIF
14:12 This PDF is an NES MD5 Quine

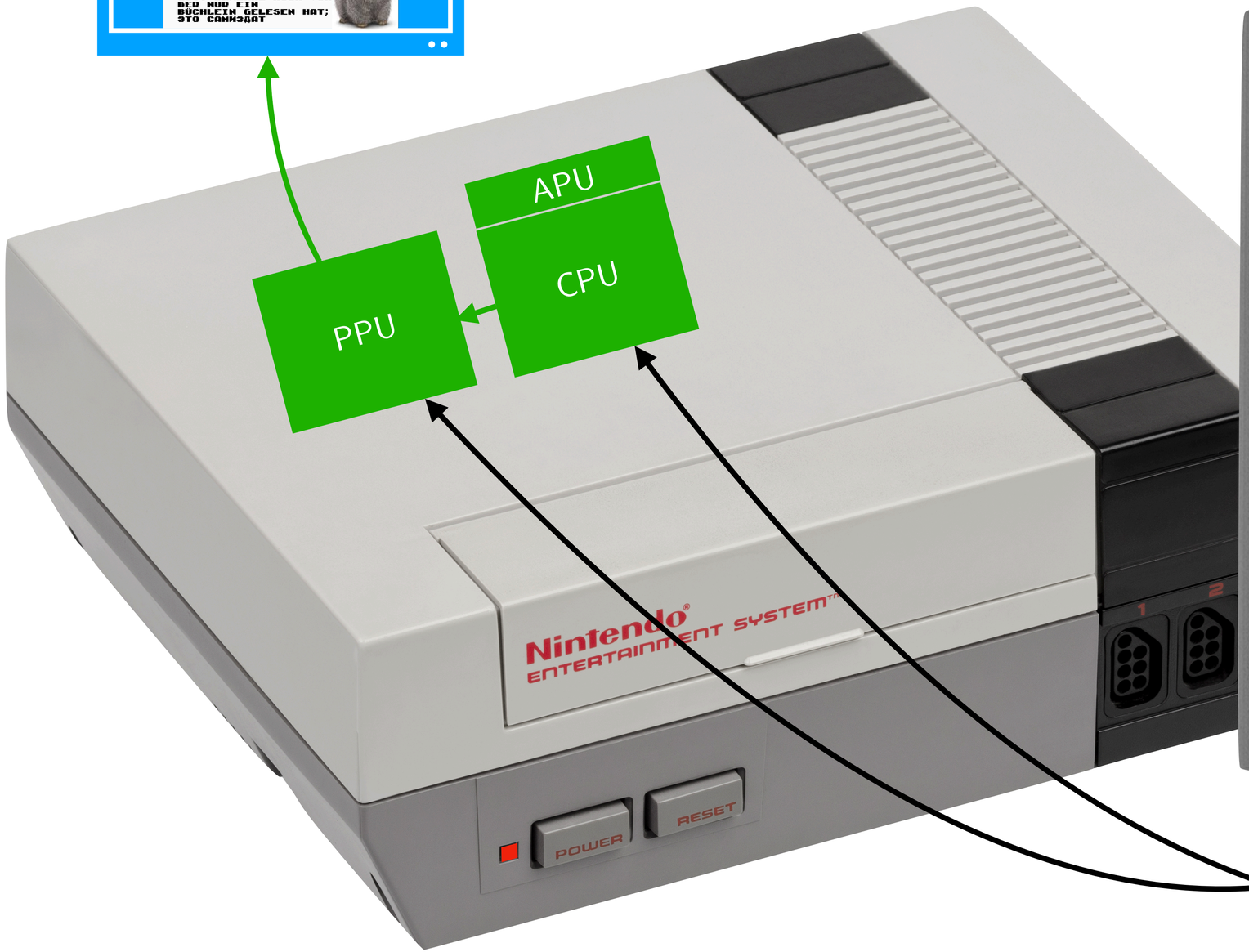
Gott bewahre mich vor jemand, der nur ein Büchlein gelesen hat; это самиздат.
The MD5 hash of this PDF is 5EAF00D25C14232555A51A50B126746C. March 20, 2017.
€ 0, $0 USD, $0 AUD, 10s 6d GBP, 0 RSD, 0 SEK, $50 CAD, 6×10^{29} Pengő (3×10^{8} Adópengő).

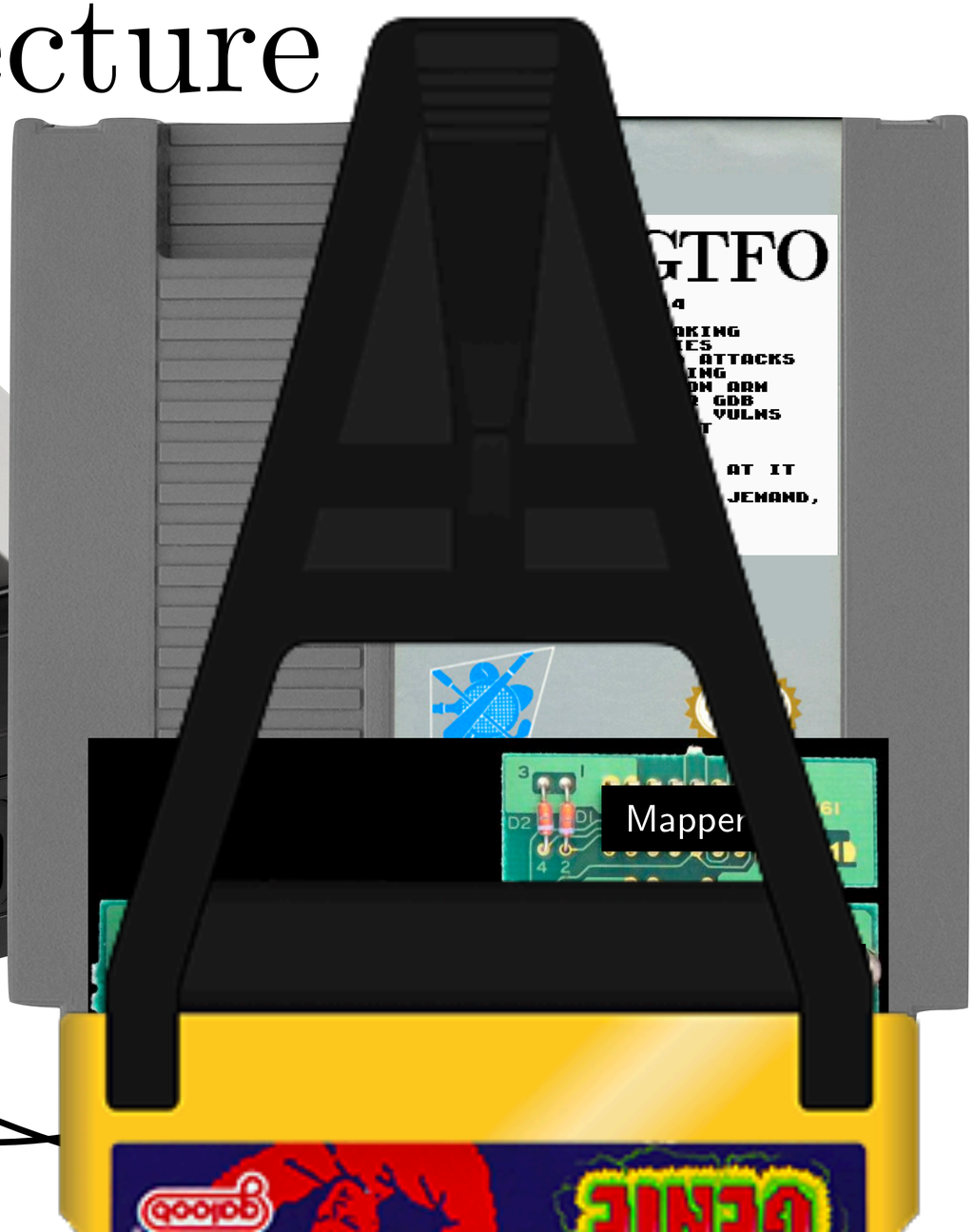
NES Architecture

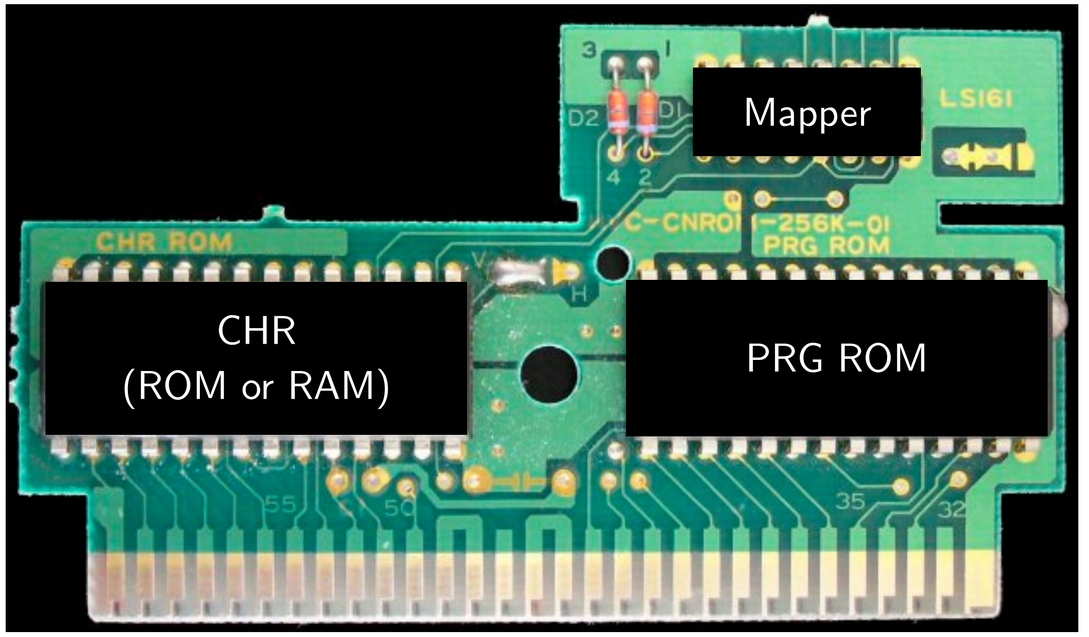
NES Architecture



NES Architecture





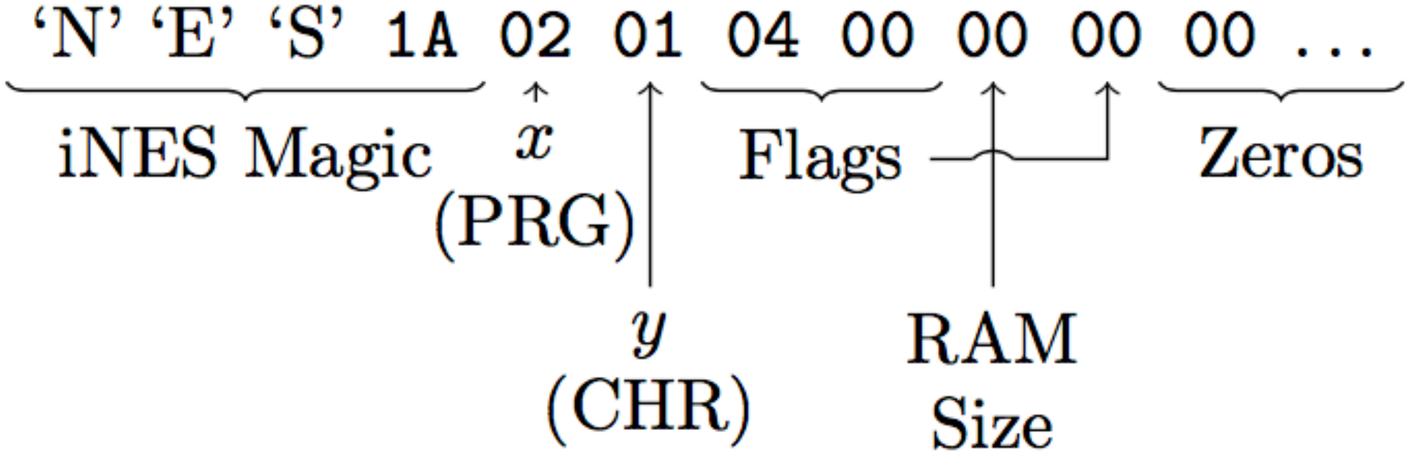


Header
16 Bytes

Trainer (Optional)
0 or 512 Bytes

PRG ROM
$x \times 16$ KiB

CHR ROM (Optional)
0 or $y \times 8$ KiB



iNES Header, including flags for a trainer

%PDF-1.5

%<D0><D4><C5><D8>

9999 0 obj

<< /Length *number of bytes remaining in the ROM* >>

stream

zeros for the remainder of the 512 Trainer bytes

the remainder of the iNES ROM

endstream

endobj

the remainder of the PDF

PoC||GTFO

ISSUE 0X14

GOTT BEWAHRE MICH VOR JEMAND,
DER NUR EIN
BÜCHLEIN GELESEN HAT;
ЭТО САМИЗДАТ

MD5: 5E AF 00 D2 5C 14 23 25
55 A5 1A 50 B1 26 74 6C

PoC||GTFO

ISSUE 0X14

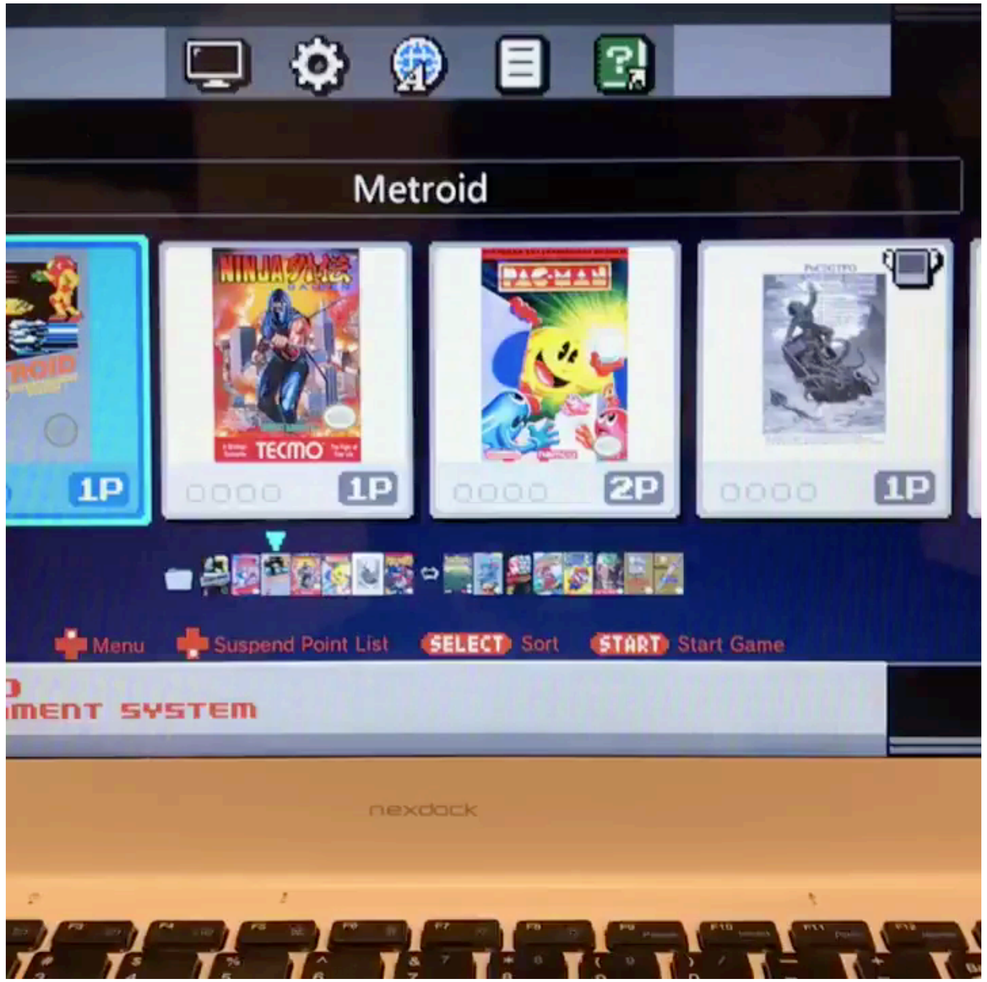
GO[illegible]BEWAHRE MICH VOR JEMAND,
[illegible]NUR EIN
[illegible]CHLEIN GELESEN HAT;
[illegible]TO САМИЗДАТ

MD5: 5E AF 00 D2 5C 14 23 25
55 A5 1A 50 B1 26 74 6C

Requires 32,768 Bytes!

ShambaliOmnics Unite
@CyberShambles

Now with music #pocorgtfo 0x14 on classic nes mini cc/ @travisgoodspeed @ESultanik @angealbertini



7:37 AM - 22 Mar 2017

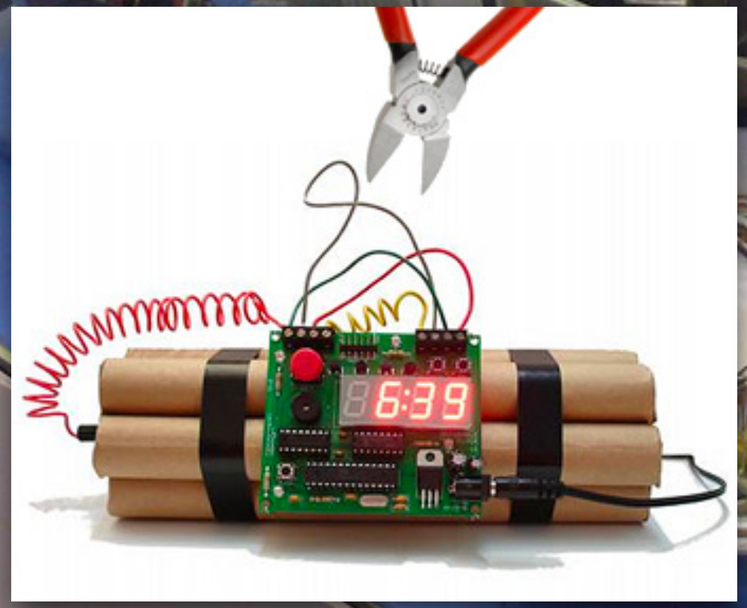
25 Retweets **25** Likes

NNSA

National Nuclear Security Administration

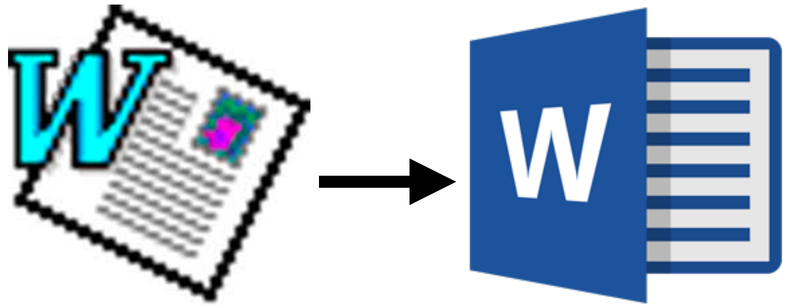
3,000,000 Square Feet
(almost 2x the size of the
Tesla Gigafactory)

1949–2014


6:39

Preserved external research.

(blog ⇒ PDF)



PDF/Git Polyglot

```
$ git bundle
```


Git Bundle Signature
v2 git bundle ↩
3aa340a2e3d125ab6703e5c9bdfede2054a9c0c5 refs/heads/master ↩
3aa340a2e3d125ab6703e5c9bdfede2054a9c0c5 refs/remotes/origin/master ↩
4146cfe2fe9249fc14623f832587efe197ef5d2d refs/stash ↩
babdda4735ef164b7023be3545860d8b0bae250a HEAD ↩
↩
Digest
PACK... ????????????
Git Packfile

Git Bundle Signature

```
# v2 git bundle ↩

3aa340a2e3d125ab6703e5c9bdfede2054a9c0c5 refs/heads/master ↩

3aa340a2e3d125ab6703e5c9bdfede2054a9c0c5 refs/remotes/origin/master ↩

4146cfe2fe9249fc14623f832587efe197ef5d2d refs/stash ↩

babdda4735ef164b7023be3545860d8b0bae250a HEAD ↩

↩

PACK...
```

Digest

Git Packfile

git / git

Watch 1,795 | Star 20,012 | Fork 11,619

Code | Pull requests 106 | Insights

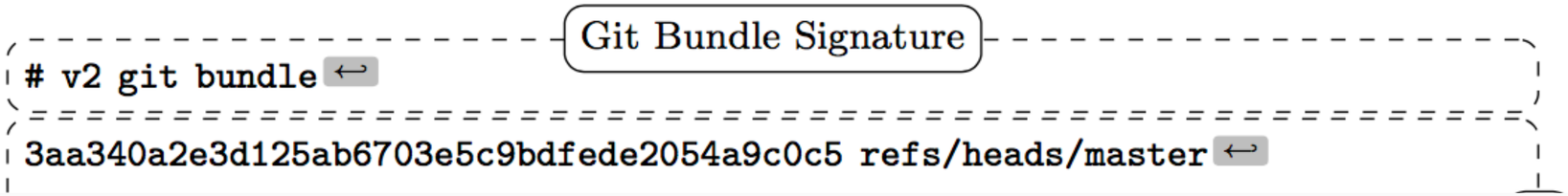
Branch: master ▾ | git / Documentation / technical / pack-format.txt | Find file | Copy path

tacker66 The name of the hash function is "SHA-1", not "SHA1" — d5fa1f1 on Apr 15, 2013

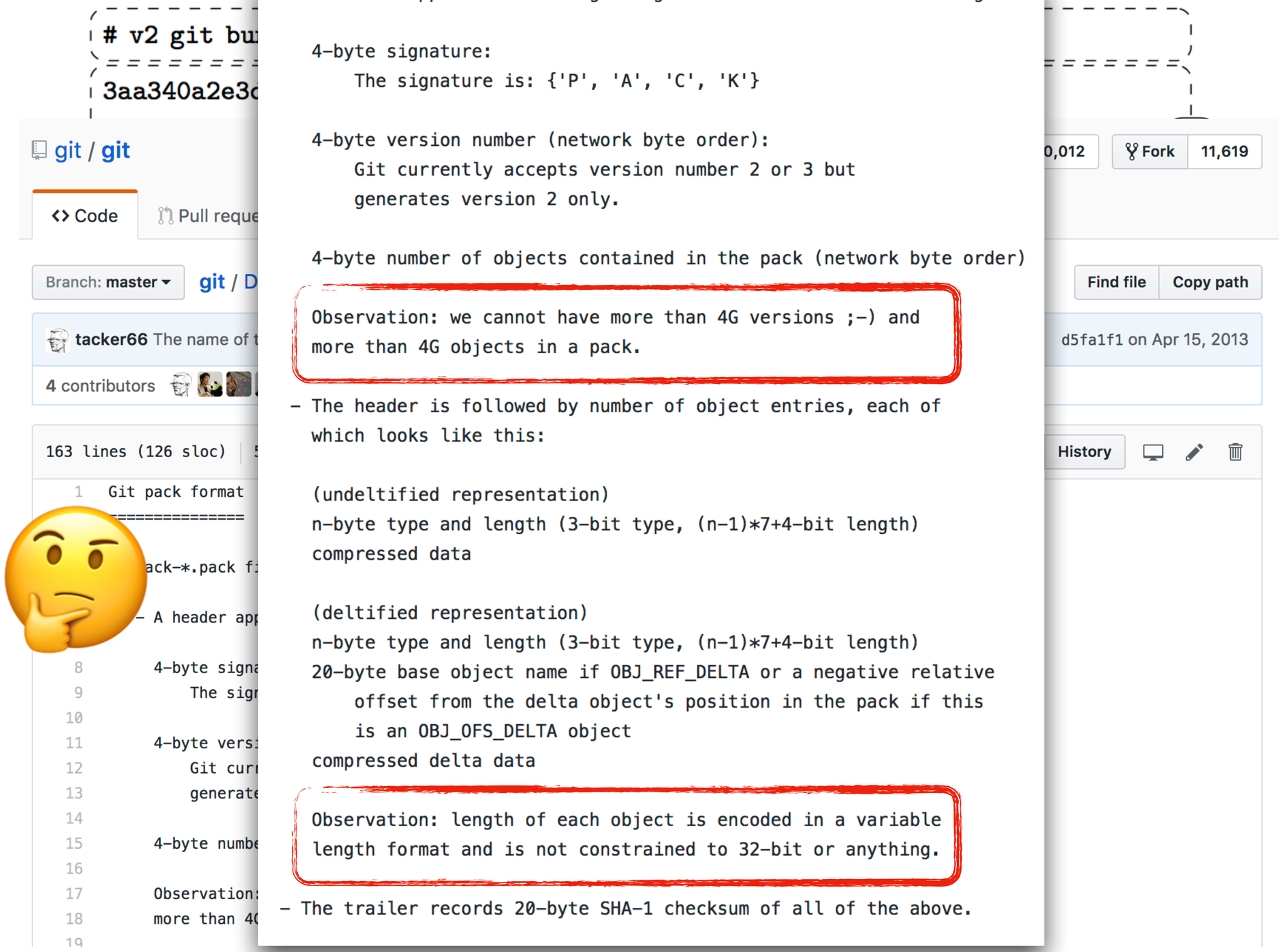
4 contributors

163 lines (126 sloc) | 5.54 KB | Raw | Blame | History

```
Git pack format
===============

== pack-*.pack files have the following format:

   - A header appears at the beginning and consists of the following:

     4-byte signature:
         The signature is: {'P', 'A', 'C', 'K'}

     4-byte version number (network byte order):
         Git currently accepts version number 2 or 3 but
         generates version 2 only.

     4-byte number of objects contained in the pack (network byte order)

     Observation: we cannot have more than 4G versions ;-) and
     more than 4G objects in a pack.
```




```
Git pack format
===============

== pack-*.pack files have the following format:

   - A header appears at the beginning and consists of the following:

     4-byte signature:
         The signature is: {'P', 'A', 'C', 'K'}

     4-byte version number (network byte order):
         Git currently accepts version number 2 or 3 but
         generates version 2 only.

     4-byte number of objects contained in the pack (network byte order)

     Observation: we cannot have more than 4G versions ;-) and
     more than 4G objects in a pack.
```


- A header appears at the beginning and consists of the following:
4-byte signature:
The signature is: {'P', 'A', 'C', 'K'}
4-byte version number (network byte order):
Git currently accepts version number 2 or 3 but
generates version 2 only.
4-byte number of objects contained in the pack (network byte order)
Observation: we cannot have more than 4G versions ;-) and
more than 4G objects in a pack.
- The header is followed by number of object entries, each of
which looks like this:
(undeltified representation)
n-byte type and length (3-bit type, (n-1)*7+4-bit length)
compressed data
(deltified representation)
n-byte type and length (3-bit type, (n-1)*7+4-bit length)
20-byte base object name if OBJ_REF_DELTA or a negative relative
offset from the delta object's position in the pack if this
is an OBJ_OFS_DELTA object
compressed delta data
Observation: length of each object is encoded in a variable
length format and is not constrained to 32-bit or anything.
- The trailer records 20-byte SHA-1 checksum of all of the above.

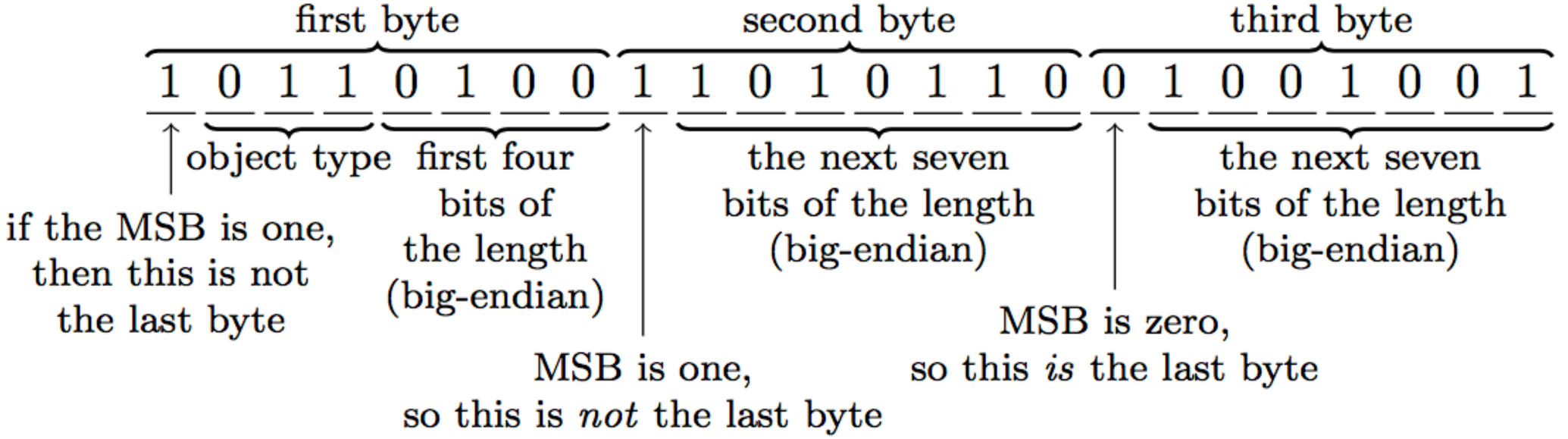
‘P’ ‘A’ ‘C’ ‘K’ 00 00 00 02 # objects

magic version big-endian 4 byte int

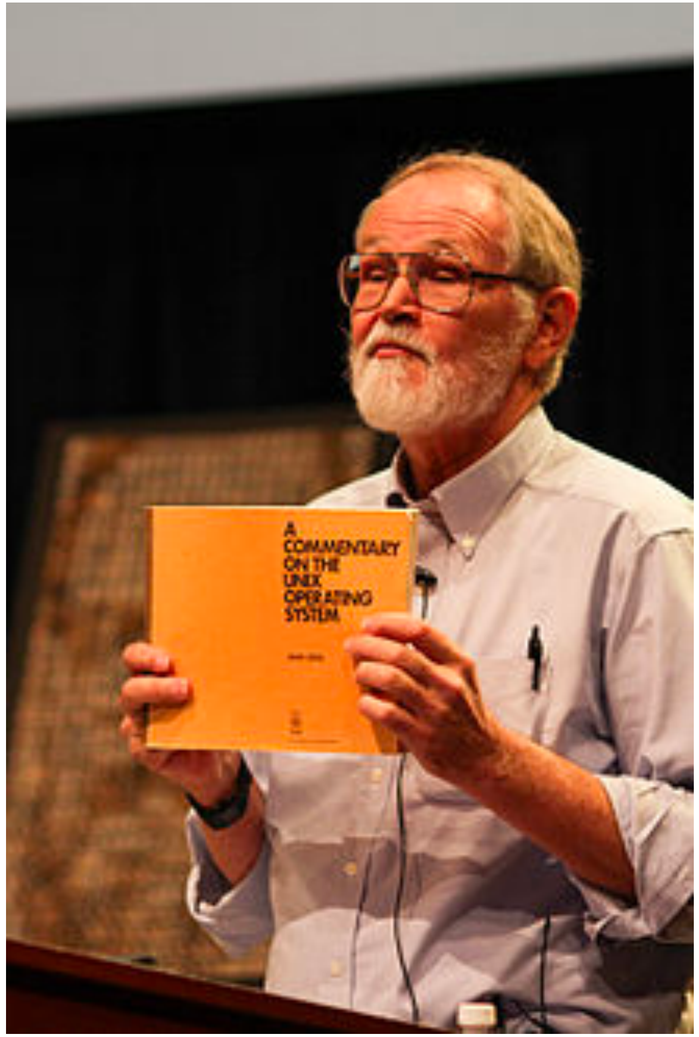
one data chunk for each object

20-byte SHA-1 of all the previous data in the pack

Data chunk: encoded *uncompressed* length followed by zlib-compressed data



Git Plumbing




```
$ git pull
```

Is equivalent to

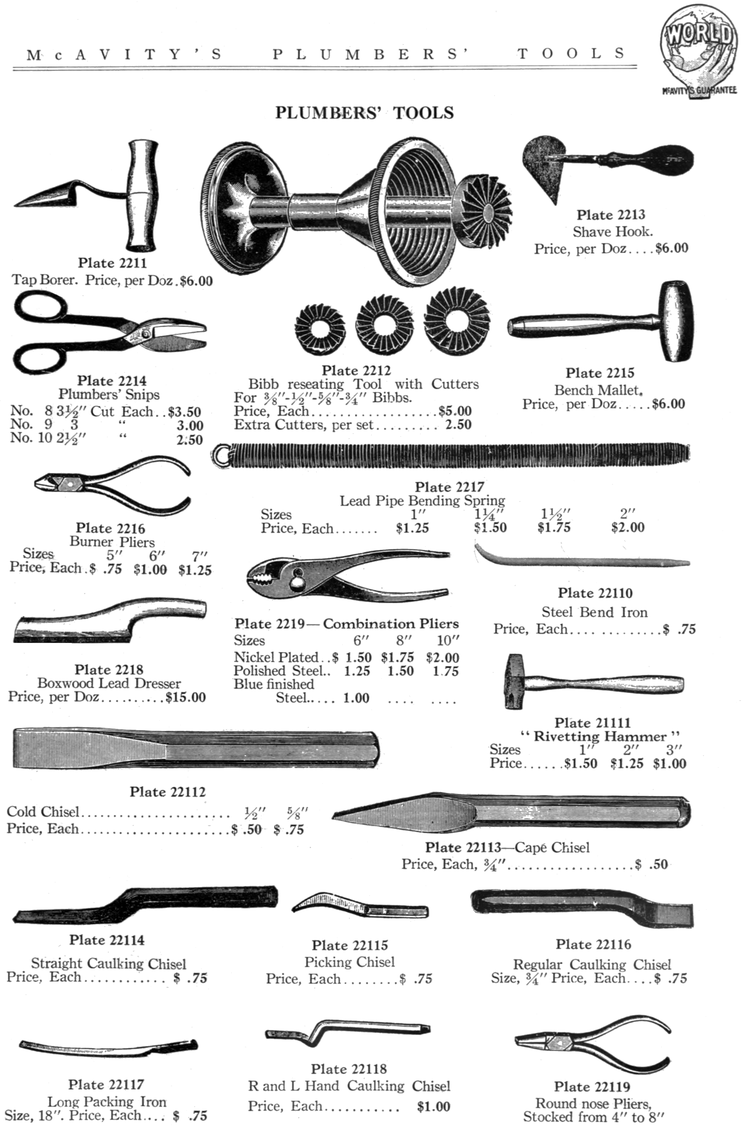
```
$ git fetch && git merge
```

Likewise,

```
$ git bundle
```

delegates to

```
$ git pack-objects
```



bundle.c

```
argv_array_pushl(&pack_objects.args,
                 "pack-objects", "--all-progress-implied",
                 "--compression=0",
                 "--stdout", "--thin", "--delta-base-offset",
NULL);
```

```
$ export PATH=/path/to/patched/git:$PATH
$ git init
$ git add article.pdf
$ git commit article.pdf -m "added"
$ git bundle create PDFGitPolyglot.pdf -all
```

https://github.com/ESultanik/PDFGitPolyglot

Our Hopes, Deflated

Maximum Size of a DEFLATE Block: 65,535 Bytes

PACK^@^@^@^B^@^@^A°µ¬´^Ax^A^@^@S#iÜ%PDF-1.4
%ÐÔÅØ
6 0 obj
<<
/Length 61337
/Filter /FlateDecode
>>
stream
PDF Object Byte Stream
endstream
endobj
7 0 obj
<<
/Length 1234
/Filter /FlatDecode
>>
stream

Our Hopes, Deflated

Maximum Size of a DEFLATE Block: 65,535 Bytes

```
PACK^@^@^@B^@^@^A°µ¬´^Ax^A^@^S#iÜ%PDF-1.4
%ÐÔÅØ
6 0 obj
<<
/Length 61337
/Filter /FlateDecode
>>
stream
```

PDF Object `00 FF FF 00 00` *Byte Stream*

```
endstream
endobj
7 0 obj
<<
/Length 1234
/Filter /FlatDecode
>>
stream
```

Our Hopes, Deflated

Maximum Size of a DEFLATE Block: 65,535 Bytes

```
PACK^@^@^@^B^@^@^A°µ¬´^Ax^A^@^@S#iÜ%PDF-1.4
%ÐÔÅØ
6 0 obj
<<
/Length 61337
/Filter /FlateDecode
>>
stream
```
PDF Object Byte Stream
```
endstream
endobj
% 00 FF FF 00 00
7 0 obj
<<
/Length 1234
/Filter /FlatDecode
>>
```

Remember to update the SHA1 hash!

Breaks xrefs in the inner PDF,
but most viewers are resilient!

This PDF is a Git Repository Containing its Own LaTeX Source and a Copy of Itself

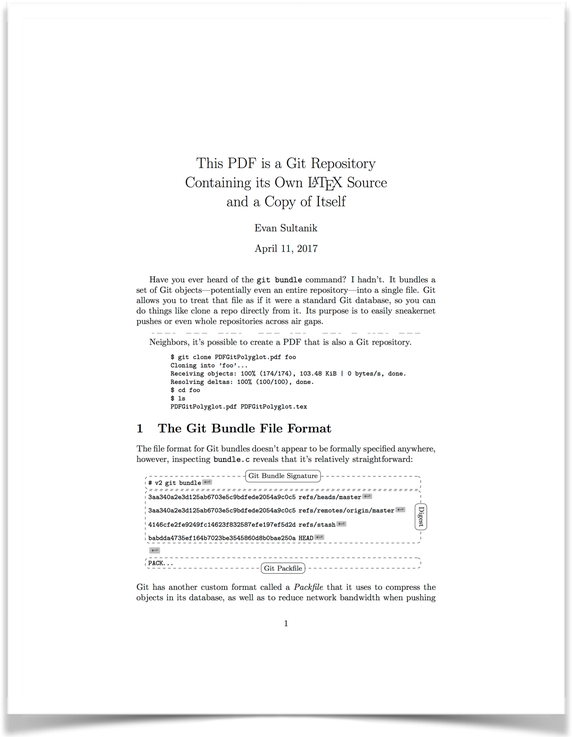
Evan Sultanik

April 11, 2017

Have you ever heard of the `git bundle` command? I hadn't. It bundles a set of Git objects—potentially even an entire repository—into a single file. Git allows you to treat that file as if it were a standard Git database, so you can do things like clone a repo directly from it. Its purpose is to easily sneakernet pushes or even whole repositories across air gaps.

Neighbors, it's possible to create a PDF that is also a Git repository.

PDF/Git Polyglot



This PDF is a Git Repository
Containing its Own LaTeX Source
and a Copy of Itself

Evan Sultanik

April 11, 2017

Have you ever heard of the `git bundle` command? I hadn't. It bundles a set of Git objects—potentially even an entire repository—into a single file. Git allows you to treat that file as if it were a standard Git database, so you can do things like clone a repo directly from it. Its purpose is to easily sneakernet pushes or even whole repositories across air gaps.

Neighbors, it's possible to create a PDF that is also a Git repository.

```
$ git clone PDFGitPolyglot.pdf foo
Cloning into 'foo'...
Receiving objects: 100% (174/174), 103.48 KiB | 0 bytes/s, done.
Resolving deltas: 100% (100/100), done.
$ cd foo
$ ls
PDFGitPolyglot.pdf PDFGitPolyglot.tex
```

1 The Git Bundle File Format

The file format for Git bundles doesn't appear to be formally specified anywhere, however, inspecting `bundle.c` reveals that it's relatively straightforward:

Git Bundle Signature

```
# v2 git bundle LF
3aa340a2e3d125ab6703e5c9bdfede2054a9c0c5 refs/heads/master LF
3aa340a2e3d125ab6703e5c9bdfede2054a9c0c5 refs/remotes/origin/master LF
4146cfe2fe9249fc14623f832587efe197ef5d2d refs/stash LF
babdda4736ef164b7023be3545860d8b0bae250a HEAD LF
LF
PACK...
```

Digest

Git Packfile

Git has another custom format called a *Packfile* that it uses to compress the objects in its database, as well as to reduce network bandwidth when pushing

1

```
$ git clone PDFGitPolyglot.pdf foo
Cloning into 'foo'...
Receiving objects: 100% (174/174), 103.48 KiB | 0 bytes/s, done.
Resolving deltas: 100% (100/100), done.
$ cd foo
$ ls
PDFGitPolyglot.pdf PDFGitPolyglot.tex
```

Conclusions

- Files have no intrinsic meaning
- Polyglots aren't just a nifty parlor trick
- You can make them, too!
- Open PostScript in a VM
- PDF is broken

Homework

Check out PoC||GTFO 0x16,
which helps you reverse engineer itself

`https://www.sultanik.com/pocorgtfo/`

Acknowledgements

Ange Albertini	`@angealbertini`
Sergey Bratus	`@sergeybratus`
Travis Goodspeed	`@travisgoodspeed`
Philippe Teuwen	`@doegox`
Evan Teran	`@evan_teran`
Jacob Torrey	`@JacobTorrey`

Et pl. al.

Thanks!

@ESultanik

https://www.sultanik.com/