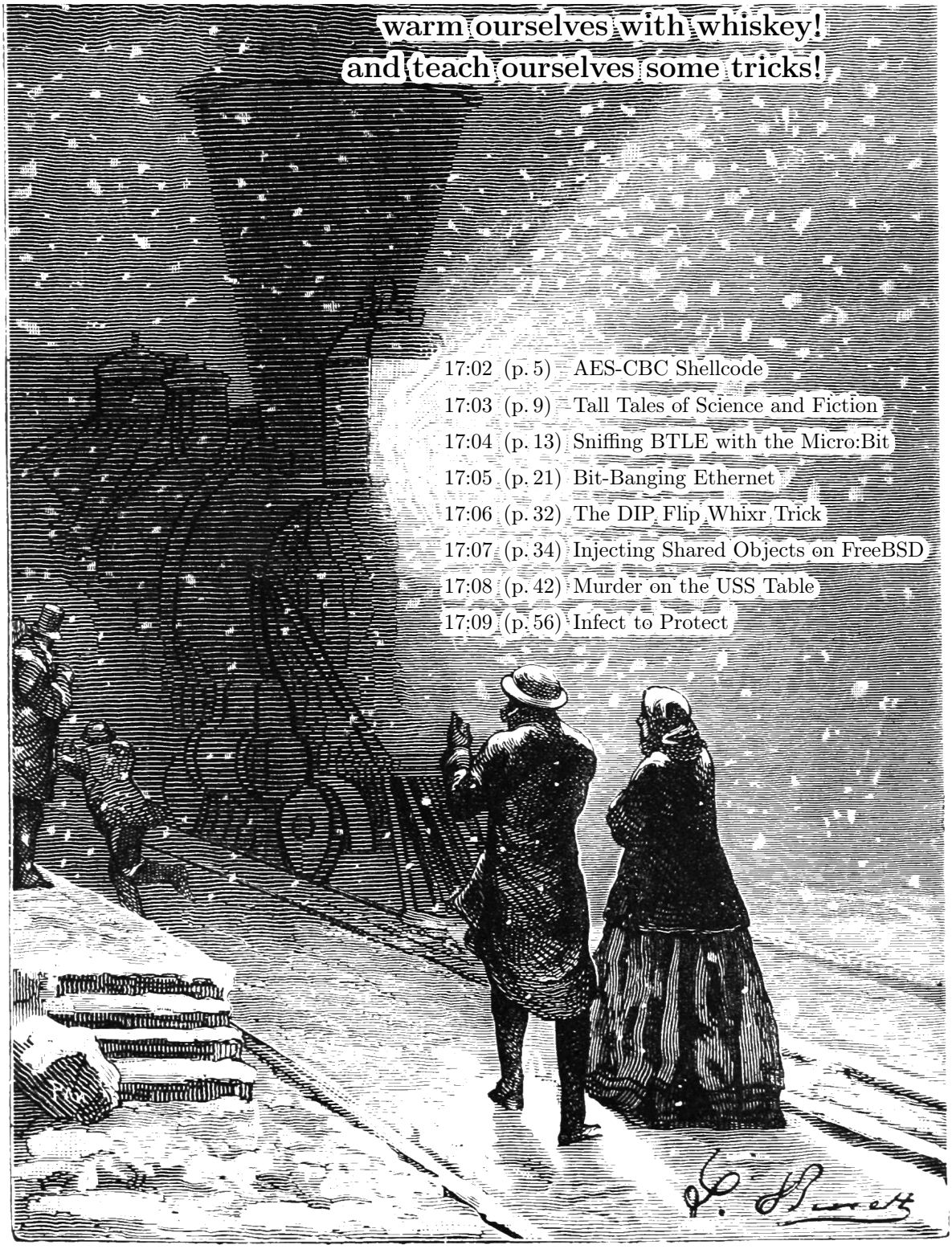
PoC||GTFO

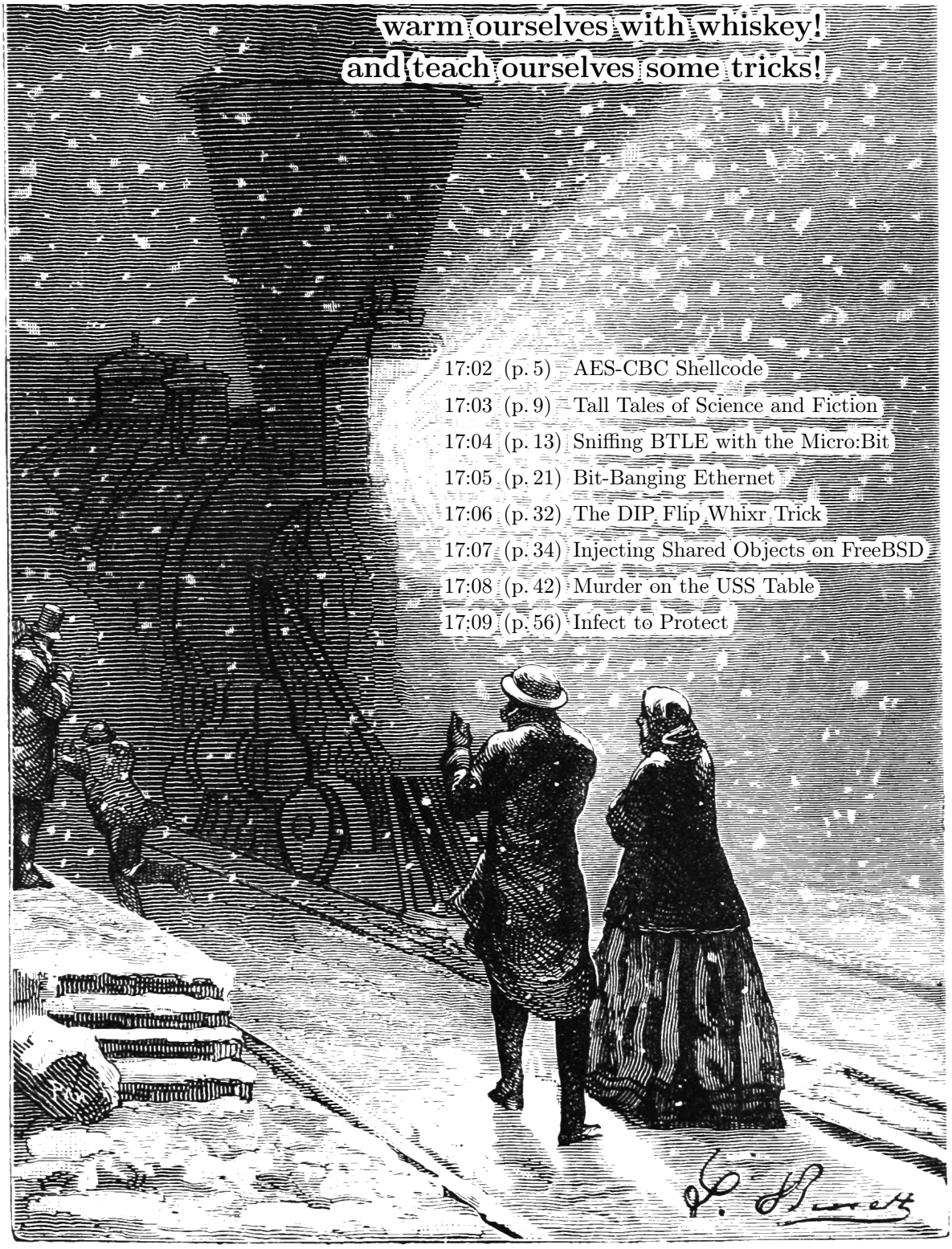
It's damned cold outside, so let's light ourselves a fire!



Des Teufels liebstes Möbelstück ist die lange Bank. Это самиздат.
Compiled on December 30, 2017. Free Radare2 license included with each and every copy!
€ 0, $0 USD, $0 AUD, 0 RSD, 0 SEK, $50 CAD, 6×10^{29} Pengő (3×10^{8} Adópengő), 100 JPC.

PoC||GTFO

It's damned cold outside, so let's light ourselves a fire!



Des Teufels liebstes Möbelstück ist die lange Bank. Это самиздат.
Compiled on December 30, 2017. Free Radare2 license included with each and every copy!
€ 0, $0 USD, $0 AUD, 0 RSD, 0 SEK, $50 CAD, 6×10^{29} Pengő (3×10^{8} Adópengő), 100 JPC.

Legal Note: Please make an extra copy of this scientific journal, by laserjet or by typewriter самиздат, and give it away. Give it to a friend, leave it in the magazine rack at the doctor's office, or hide it inside a good technical book at your local library.

Reprints: Bitrot will burn libraries with merciless indignity that even Pets Dot Com didn't deserve. Please mirror—don't merely link!—`pocorgtfo17.pdf` and our other issues far and wide, so our articles can help fight the coming flame deluge. We like the following mirrors.

https://unpack.debug.su/pocorgtfo/ https://pocorgtfo.hacke.rs/
https://www.alchemistowl.org/pocorgtfo/ https://www.sultanik.com/pocorgtfo/

Technical Note: This file, `pocorgtfo17.pdf`, is valid as a PDF file, a ZIP file, and as firmware for the Apollo Guidance Computer. We the editors do not recommend it for use in space navigation, and we warn our fine readers that replacing a spaceship's navigational firmware before a flight would be a joke in extremely poor taste.

```
# Start the emulator GUI on localhost:19697
  (cd VirtualAGC/Resources && ../bin/yaDSKY2) &
# Assemble the firmware image.
  yaYUL pocorgtfo17.pdf
# Engage!
  yaAGC --nodebug pocorgtfo17.pdf.bin
```

Cover Art: As with the previous issue, the cover illustration from this release is a Hildibrand engraving of a painting by Léon Benett that was first published in *Le tour du monde en quatre-vingts jours* by Jules Verne in 1873.

Printing Instructions: Pirate print runs of this journal are most welcome! PoC||GTFO is to be printed duplex, then folded and stapled in the center. Print on A3 paper in Europe and Tabloid (11" x 17") paper in Samland, then fold to get a booklet in A4 or Letter size. Secret volcano labs in Canada may use P3 (280 mm x 430 mm) if they like, folded to make P4. The outermost sheet should be on thicker paper to form a cover.

```
# This is how to convert an issue for duplex printing.
sudo apt-get install pdfjam
pdfbook --short-edge --vanilla --paper a3paper pocorgtfo17.pdf -o pocorgtfo17-book.pdf
```


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 Bus Driver	Ryan Speers
with the good assistance of	
Samizdat Postmaster	Nick Farr

17:01 I thought I turned it on, but I didn't.

Neighbors, please join me in reading this eighteenth release of the International Journal of Proof of Concept or Get the Fuck Out, a friendly little collection of articles for ladies and gentlemen of distinguished ability and taste in the field of reverse engineering and the study of weird machines. This release is a gift to our fine neighbors in Leipzig and Washington, D.C.

If you are missing the first seventeen issues, we suggest asking a neighbor who picked up a copy of the first in Vegas, the second in São Paulo, the third in Hamburg, the fourth in Heidelberg, the fifth in Montréal, the sixth in Las Vegas, the seventh from his parents' inkjet printer during the Thanksgiving holiday, the eighth in Heidelberg, the ninth in Montréal, the tenth in Novi Sad or Stockholm, the eleventh in Washington D.C., the twelfth in Heidelberg, the thirteenth in Montréal, the fourteenth in São Paulo, San Diego, or Budapest, the fifteenth in Canberra, Heidelberg, or Miami, the sixteenth release in Montréal, New York, or Las Vegas, or the seventeenth release in São Paulo or Budapest.

After our paper release, and only when quality control has been passed, we will make an electronic release named `pocorgtfo17.pdf`. It is a valid PDF document and a ZIP file filled with fancy papers and source code. It is also a valid program for the Apollo Guidance Computer, which will run in the VirtualAGC emulator.

As you'll recall from PoC||GTFO 3:11, AES in CBC mode allows you to flip bits of the initialization vector to flip bits of the first cleartext block. On page 5, Albert Spruyt and Niek Timmers share some handy tricks for using a similar property: by flipping bits of one block's ciphertext you can also flip blocks of the subsequent ciphertext block after decryption. In this manner, they can sacrifice half of the blocks by flipping their bits to control the other half, loading shellcode into the cleartext of an encrypted ARM image for which they have no key.

Our own Pastor Laphroaig has a sermon for you on page 9, concerning the good ol' days of juvenile science fiction, when chemistry sets were dangerous and Dr. Watson trusty pistol was always at hand.

Software defined radios and radios built from custom hardware can receive damned near anything these days, but some of the most clever radio hacking involves firmware patches to existing, commodity radios. On page 13, Damien Cauquil shows us how to write custom firmware for the nRF51 chip in the BBC Micro:Bit to sniff an ongoing Bluetooth Low Energy connection, without previously knowing the hop interval, increment, or even the channel map.

Speaking of PHY layer tricks, what does a clever neighbor do when he hasn't got a hardware PHY? For Ethernet, Andrew Zonenberg simply bitbangs it from an old Spartan-6 FPGA and the right resistors. Page 21.

When assembling hardware, sometimes it can be ambiguous whether a chip is inserted one way, or rotated one hundred and eighty degrees from that way. On page 32, Joe Grand shares with us a DIP-8 design that selectively re-adjusts itself to having the chip rotated. Build your PCB by the ferric chloride method with a 0.1" DIP socket for proper nostalgia.

Back in the good ol' days, folks would share hooking techniques over a pint of good ale. Now that pints have as few as eight ounces, and some jerk ranting about Bitcoin ruins all our conversations, it's nice to read that Shawn Webb has been playing with methods for hooking functions in FreeBSD processes through unprivileged `ptrace()` debugging. Page 34.

Page 42 features a gumshoe detective novella, one in which Soldier of Fortran hangs out his neon sign and teams up with Bigendian Smalls to create the niftiest EBCDIC login screen for his z/OS mainframe.

Leandro Pereira has some clever tricks on page 56 for injecting additional code into preexisting ELF files to enable defensive features through `seccomp-bpf`.

On page 60, the last page, we pass around the collection plate. Our church has no interest in bitcoins or wooden nickels, but we'd love your donation of a reverse engineering story. Please send one our way.