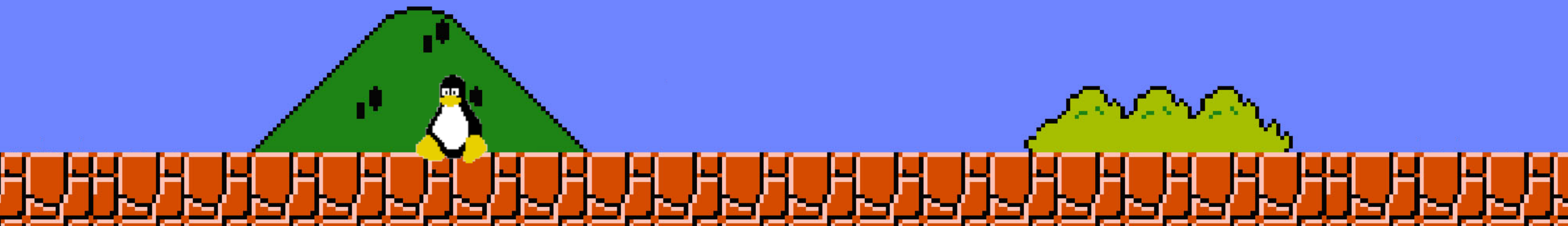
×00 WORLD 1-1

THE POWER OF PHYSICAL ACCESS

IAN TRENT



https://github.com/nulvox/switch-armyknife/

Ian

Not a lawyer; none of this is valid legal advice.

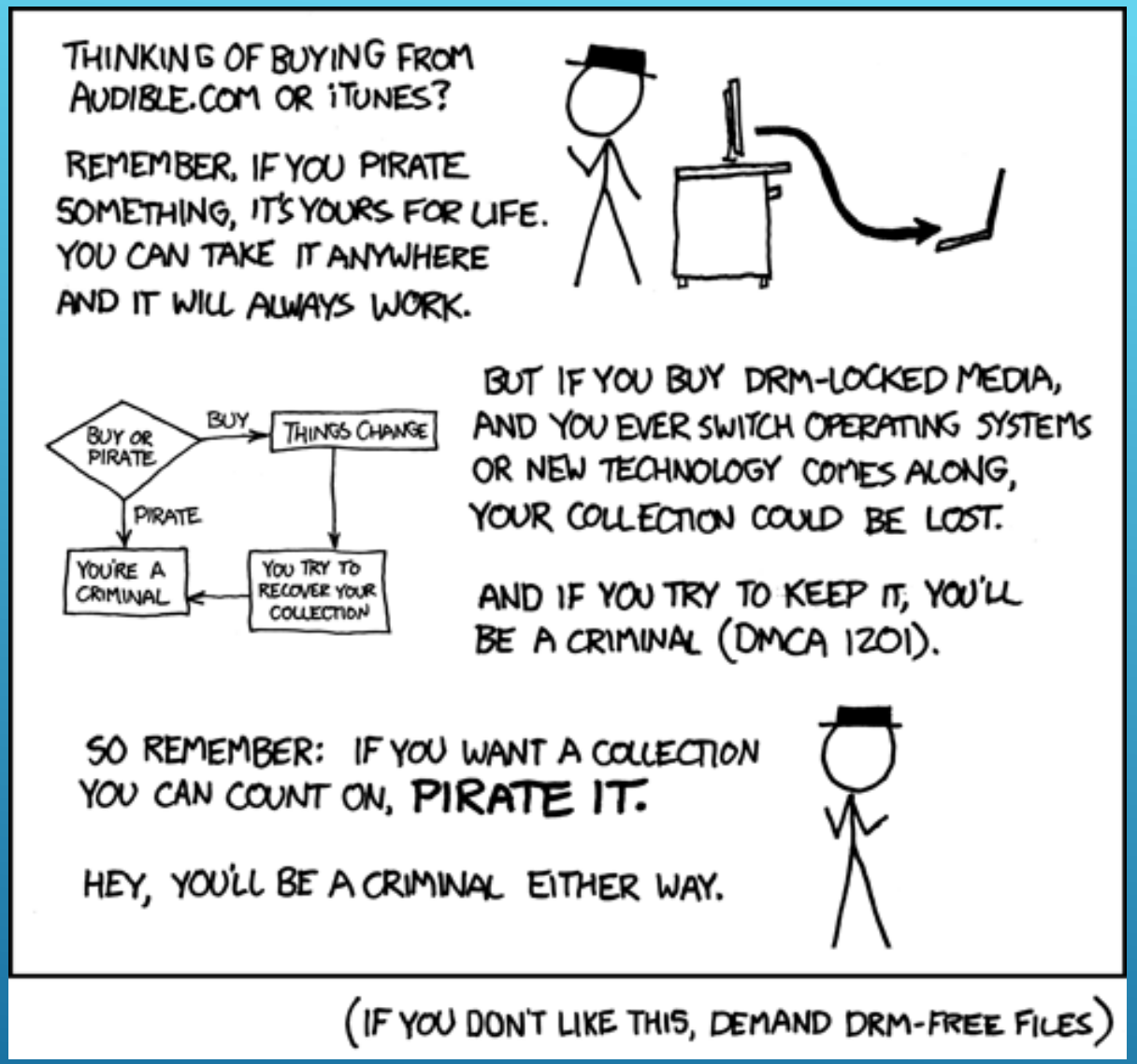
DIGITAL MILLENNIUM COPYRIGHT ACT

- Treaties with World Intellectual Property Organization in 1996
- US bill passed in 1998
- Removing DRM is illegal, even if you don't steal with the capability
- Providing links to pirated content is illegal
- Providing tools to remove DRM is illegal

ONLY THIEVES WOULD WANT TO BYPASS DRM!

(RIGHT?)

- Gobbles system resources
- Excessive permissions
- Usually calls back over the network
- WibuKey exposes vulnerabilities to Siemens ICS systems 2019
- Android binder backdoor 2017
- Denuvo leaks developer creds 2017
- Wild iPhone DRM backdoor 2016
- Sony BMG rootkit 2005



https://imgs.xkcd.com/comics/steal_this_comic.png

WHEN CAN YOU CIRCUMVENT DRM?

- For screen readers on electronic books
- For educational fair use if that circumvention is necessary
- To connect old cellphones to modern networks
- To patch vulnerabilities if you don't use it for piracy
- Fixing land vehicles you own
  - read your John Deere license
- Allowing your 3D printer to use 3rd party materials
- A few others as renewed every 3 years

Sony PSP

- Recovery mode started with pandora battery
  - Just remove a pin from the battery micro
- Tethered exploitation came later
- Followed by TIFF buffer overflows

XBOX 360

- Optical drive firmware prevented execution of unsigned discs
- Basically a digital "Keep out under penalty of law" sign

Nintendo Wii

- Started with Legend of Zelda modified saves
  - Buffer overflow in player name
  - NPC referring to you by name triggers
- Wii's digital mail service executes code after the message

Nintendo Switch

- Tegra X1 bootrom vulnerability
  - Need to press vol+,home(on the console, not the joycon),and power
- Overclocking seems to increase likelihood that your display is destroyed
- USB requires a powered hub
- Battery emergency shutoff is configured wrong without custom kernel mods
- Wifi does not work on first boot from a coldstart

Use at your own risk. I am in no way responsible for your Switch exploding, catching fire, losing LCD output, destroying the power supply, stealing your car, becoming a windigo, or sustaining any other damage you can imagine.

Embedded systems are easy to brick! You have been warned.

My process

- 3D print an RCM jig[1]
- Flash the image from painless linux [2]
- Copy a kernel that worked with my sdcard to /boot [6]
- Install qemu-aarch64 with static user[3][4]
- Enable CONFIG_BINFMT_MSC in my kernel[3][4]
- Mount the sd card
- Register aarchc bin interpreter, then chroot to the sd [3] [4]

The ritual continues

- Manually patch the drivers to set battery periph registers [5]*
  - Prevents emergency shutoff at ~60% battery
- Update pacman and install the good stuff [0]
- Copy clobbered config files from a backup of painless linux
- Push SHOFEL2 over USB [2]
- Hours of candles, chanting, and incense

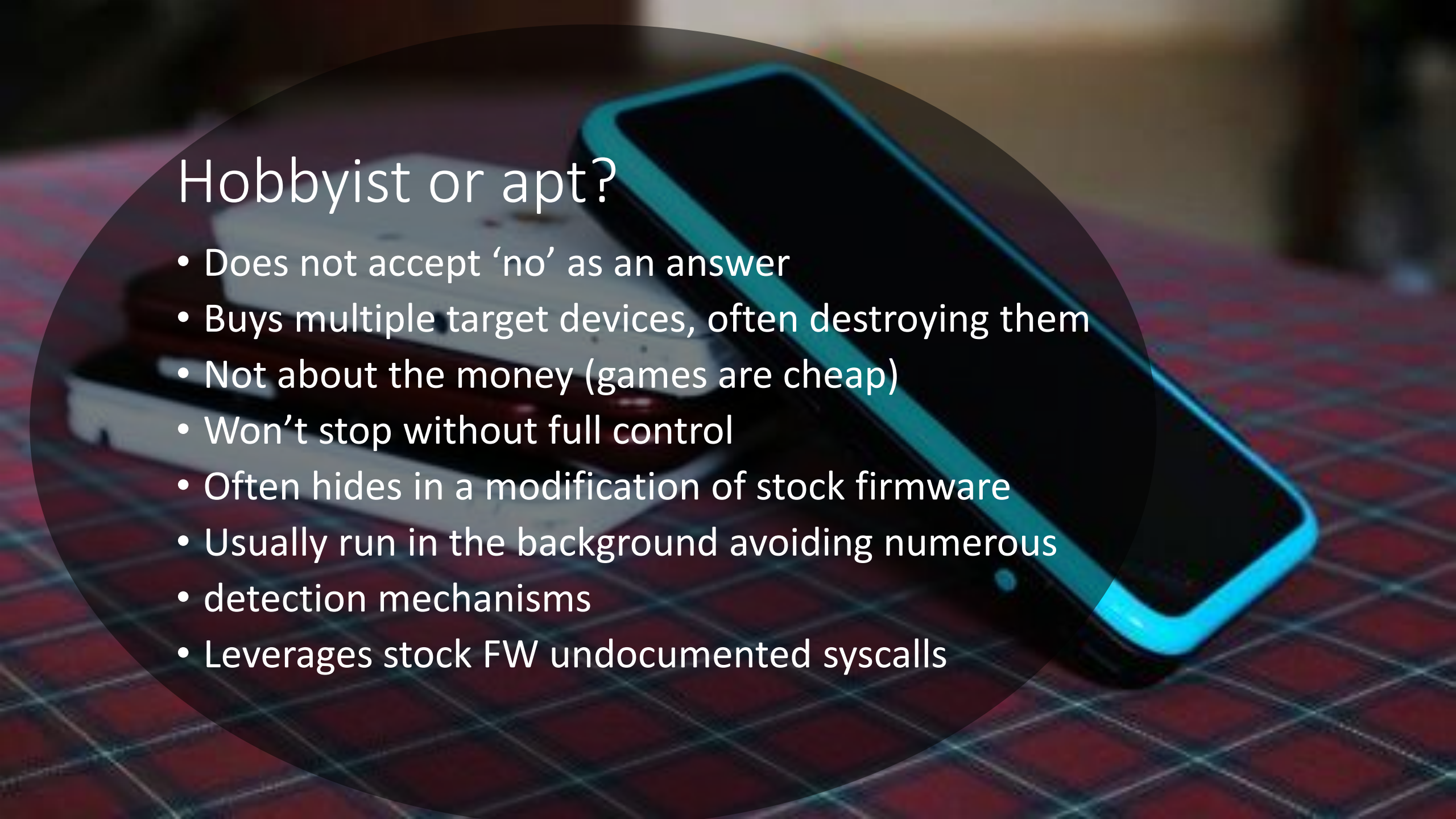
PACKAGE LIST

- Nmap
- Aircrack-ng
- Hashcat
- Wireshark
- Netcat
- Gdb
- Ettercap

- Iptables
- ebtables
- Openvpn
- Gattacker
- Numpy
- Scapy
- screen

What (probably) shouldn't do

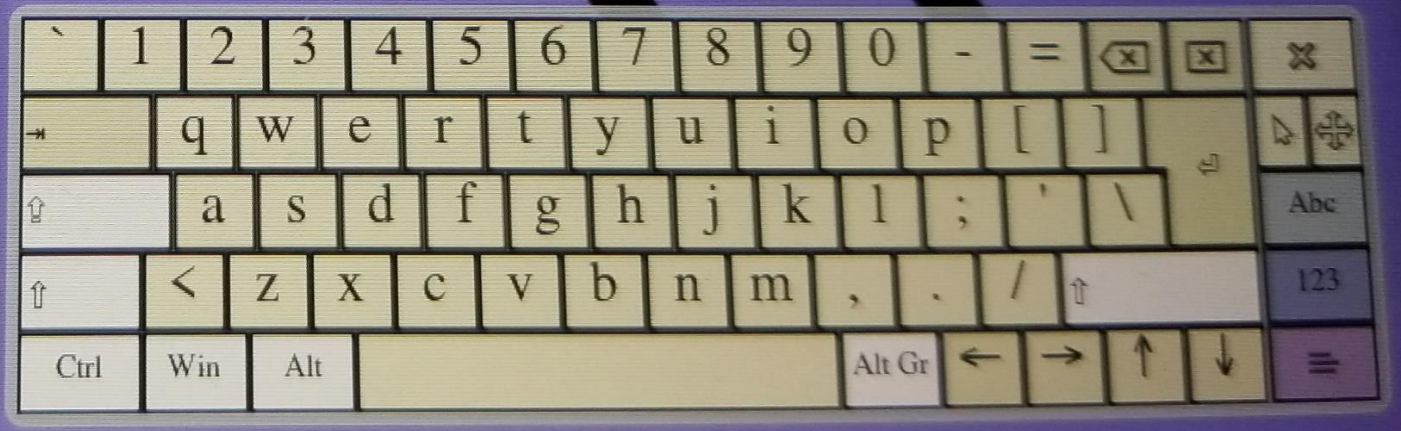
- Print an RCM jig
  - or use anything else to short pin 10
  - Soldering irons work well for this; pin 9 is gnd
- git clone https://github.com/nulvox/switch-armyknife.git
- dd if=switch-armyknife/sak.img of=/dev/{name of target SD card}
- Enter RCM mode
- Push the exploit
- Hack away!

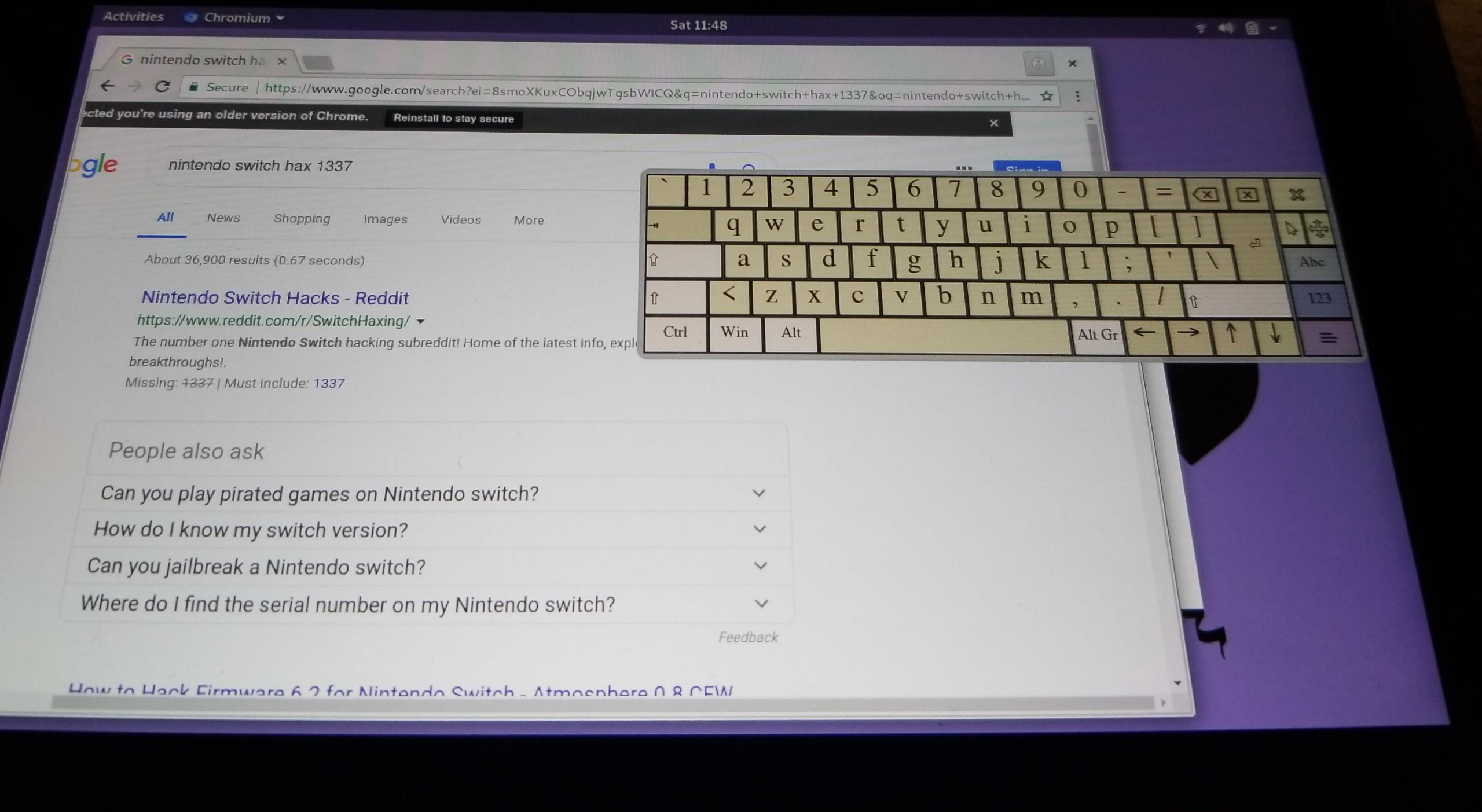


Hobbyist or apt?

- Does not accept ‘no’ as an answer
- Buys multiple target devices, often destroying them
- Not about the money (games are cheap)
- Won’t stop without full control
- Often hides in a modification of stock firmware
- Usually run in the background avoiding numerous
- detection mechanisms
- Leverages stock FW undocumented syscalls

```
  --init-eval-command=COMMAND, -iex
                  Like -ex but before loading inferior.
  --nh            Do not read ~/.gdbinit.
  --nx            Do not read any .gdbinit files in any directory.

Output and user interface control:

  --fullname      Output information used by emacs-GDB interface.
  --interpreter=INTERP
                  Select a specific interpreter / user interface
  --tty=TTY       Use TTY for input/output by the program being debugged.
  -w              Use the GUI interface.
  --nw            Do not use the GUI interface.
  --tui           Use a terminal user interface.
  --dbx           DBX compatibility mode.
  -q, --quiet, --silent
                  Do not print version number on startup.

Operating modes:

  --batch         Exit after processing options.
  --batch-silent  Like --batch, but suppress all gdb stdout output.
  --return-child-result
                  GDB exit code will be the child's exit code.
  --configuration Print details about GDB configuration and then exit.
  --help          Print this message and then exit.
  --version       Print version information and then exit.

Remote debugging options:

  -b BAUDRATE     Set serial port baud rate used for remote debugging.
  -l TIMEOUT      Set timeout in seconds for remote debugging.

Other options:

  --cd=DIR        Change current directory to DIR.
  --data-directory=DIR, -D
                  Set GDB's data-directory to DIR.

At startup, GDB reads the following init files and executes their commands:
   * system-wide init file: /etc/gdb/gdbinit

For more information, type "help" from within GDB, or consult the
GDB manual (available as on-line info or a printed manual).
Report bugs to "<http://www.gnu.org/software/gdb/bugs/>".

[alarm@alarm ~]$
```




Activities
Chromium
Sat 11:48
nintendo switch ha
Secure | https://www.google.com/search?ei=8smoXKuxCObqjwTgsbWICQ&q=nintendo+switch+hax+1337&oq=nintendo+switch+h...
ected you're using an older version of Chrome.
Reinstall to stay secure
nintendo switch hax 1337
All
News
Shopping
Images
Videos
More
About 36,900 results (0.67 seconds)
Nintendo Switch Hacks - Reddit
https://www.reddit.com/r/SwitchHaxing/
The number one Nintendo Switch hacking subreddit! Home of the latest info, expl
breakthroughs!.
Missing: 1337 | Must include: 1337
People also ask
Can you play pirated games on Nintendo switch?
How do I know my switch version?
Can you jailbreak a Nintendo switch?
Where do I find the serial number on my Nintendo switch?
Feedback
How to Hack Firmware 6.2 for Nintendo Switch - Atmosphere 0.8 CFW

FUTURE RESEARCH?

- Dock
  - Firmware RE
    - has exposed jtag headers
  - Video streaming side channel
  - Clockrate modifications
  - Use it from linux
- Switch to gentoo
  - Systemd sucks

Joycons
- Kernel drivers already exist
- 10-pin UART could add useful periphreals

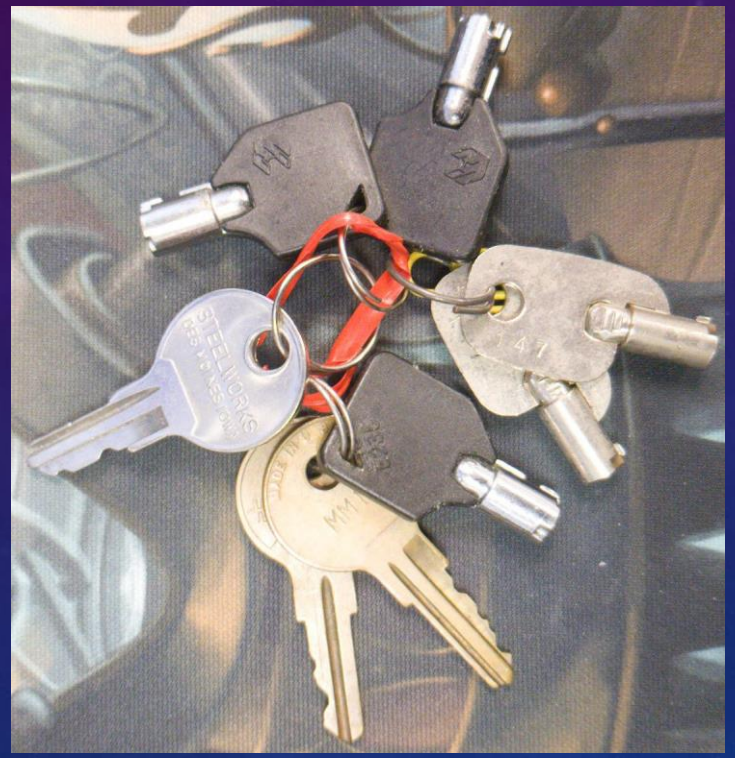
Linux kernel
- USB host power
- Enable joycons
- Wifi issues

Tegra bootrom RE
- Video streaming side channel
- Debugger hooks Linux bug fixes

WHY STOP WITH THE SWITCH?

Switch hardware capabilities:

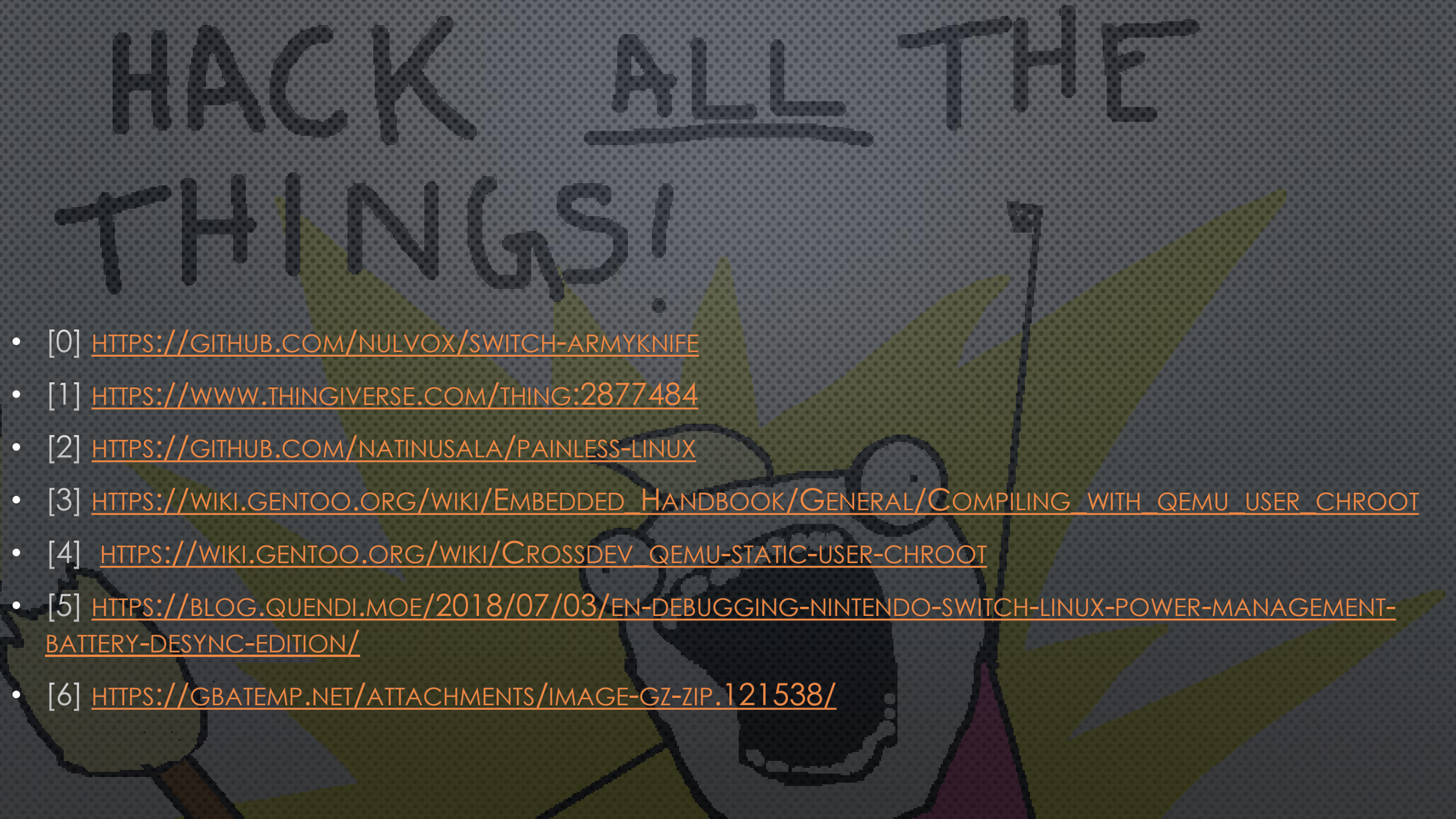
- UART
- Wifi
- BLE
- NFC
- USB (sorta)
- Capacitive touchscreen
- Accelerometers



Talk to:

- Vending machines
- CAN bus
- Building locks
- Elevators
- Smart homes
- ??????
- PROFIT!!!!

Do not hack things you don't own without explicit written permission to test from the owners.

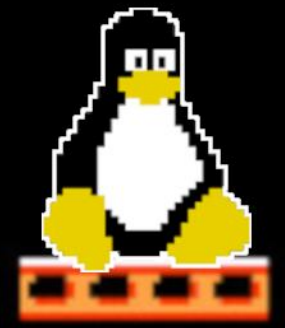


- [0] https://github.com/nulvox/switch-armyknife
- [1] https://www.thingiverse.com/thing:2877484
- [2] https://github.com/natinusala/painless-linux
- [3] https://wiki.gentoo.org/wiki/Embedded_Handbook/General/Compiling_with_qemu_user_chroot
- [4] https://wiki.gentoo.org/wiki/Crossdev_qemu-static-user-chroot
- [5] https://blog.quendi.moe/2018/07/03/en-debugging-nintendo-switch-linux-power-management-battery-desync-edition/
- [6] https://gbatemp.net/attachments/image-gz-zip.121538/

Other useful switch links

- https://github.com/CTCaer/hakate
  - Neat bootloader
- https://fail0verflow.com/blog/2018/shofel2/
  - The blog that started it all
- https://github.com/dekuNukem/Nintendo_Switch_Reverse_Engineering/blob/master/README.md
  - Great reverse engineering repo
- https://github.com/smealum
  - Smealum, the guy who drove 3DS homebrew dev is now into the switch
  - His work did not go into this, he works from HorizonOS

ANY QUESTIONS?



https://github.com/nulvox/switch-armyknife