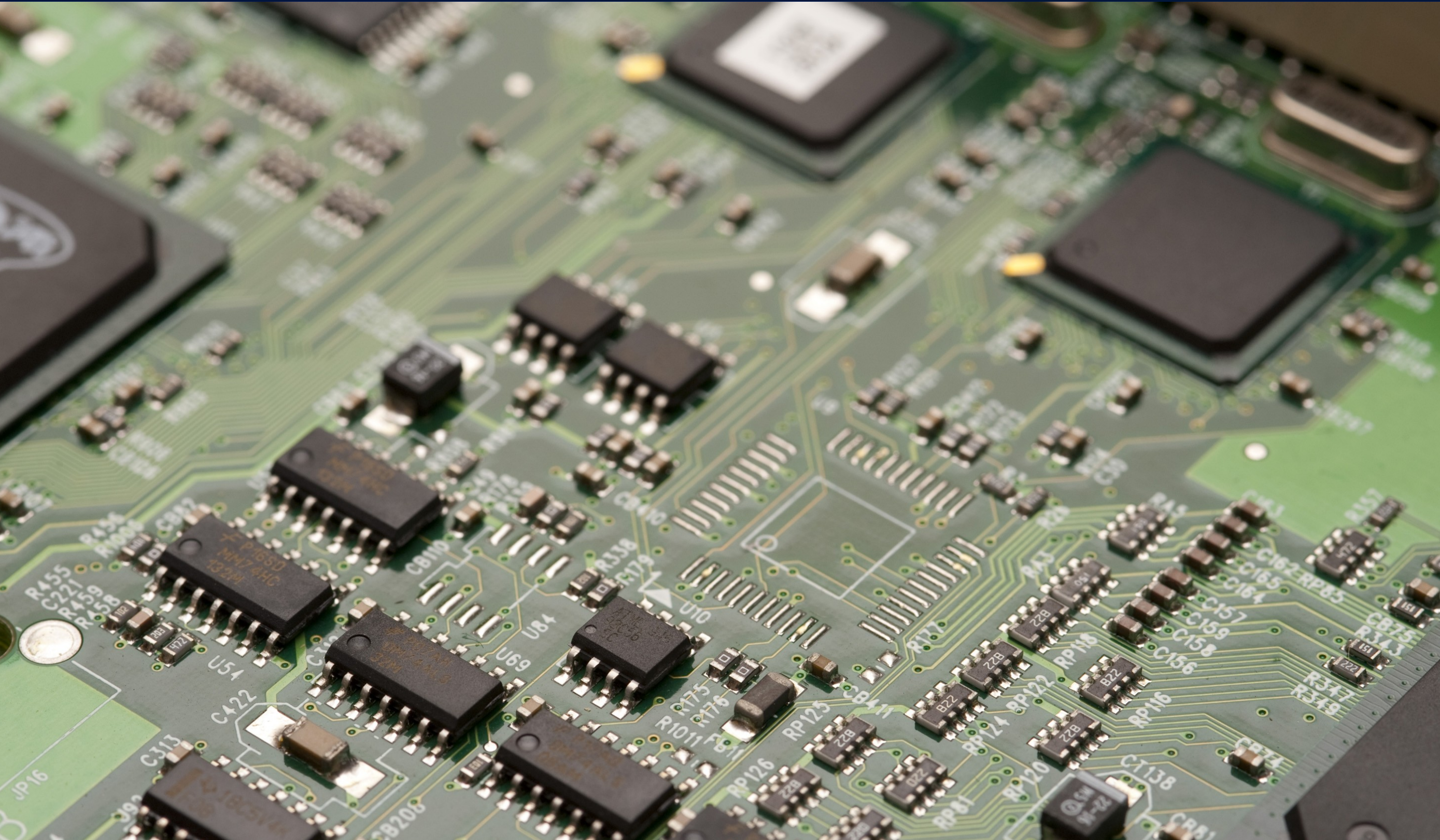
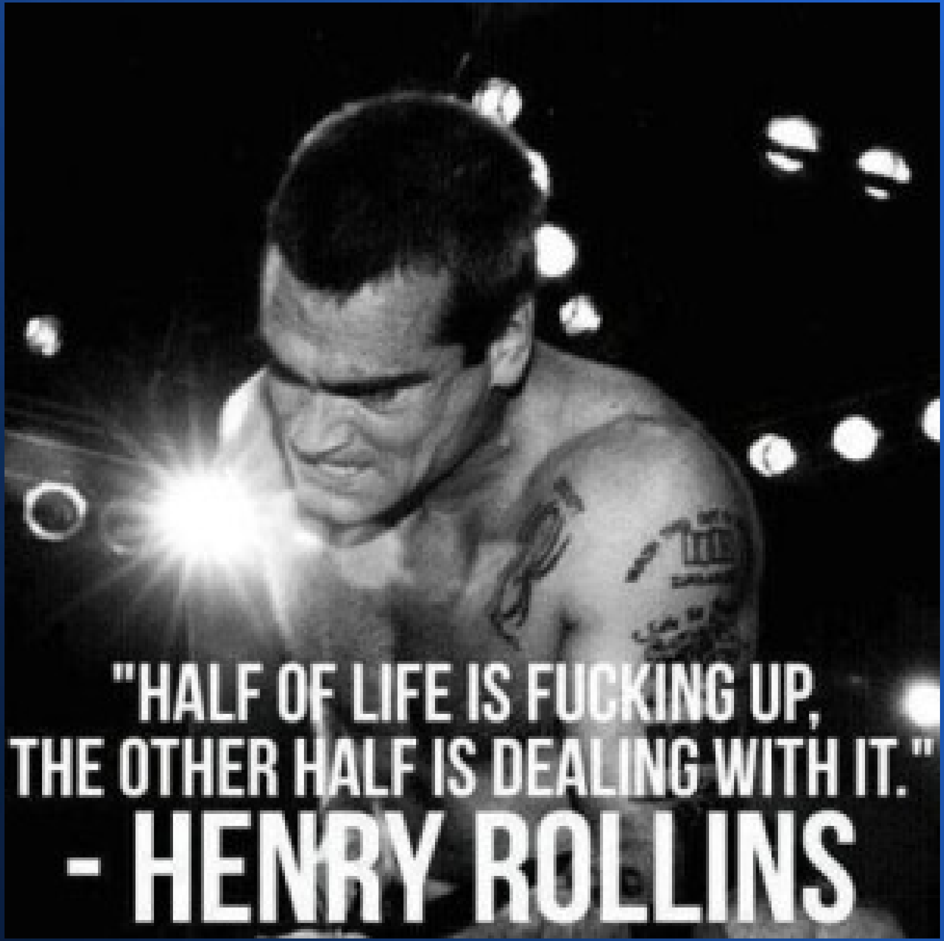
From Brick to Recovery: When devices fail



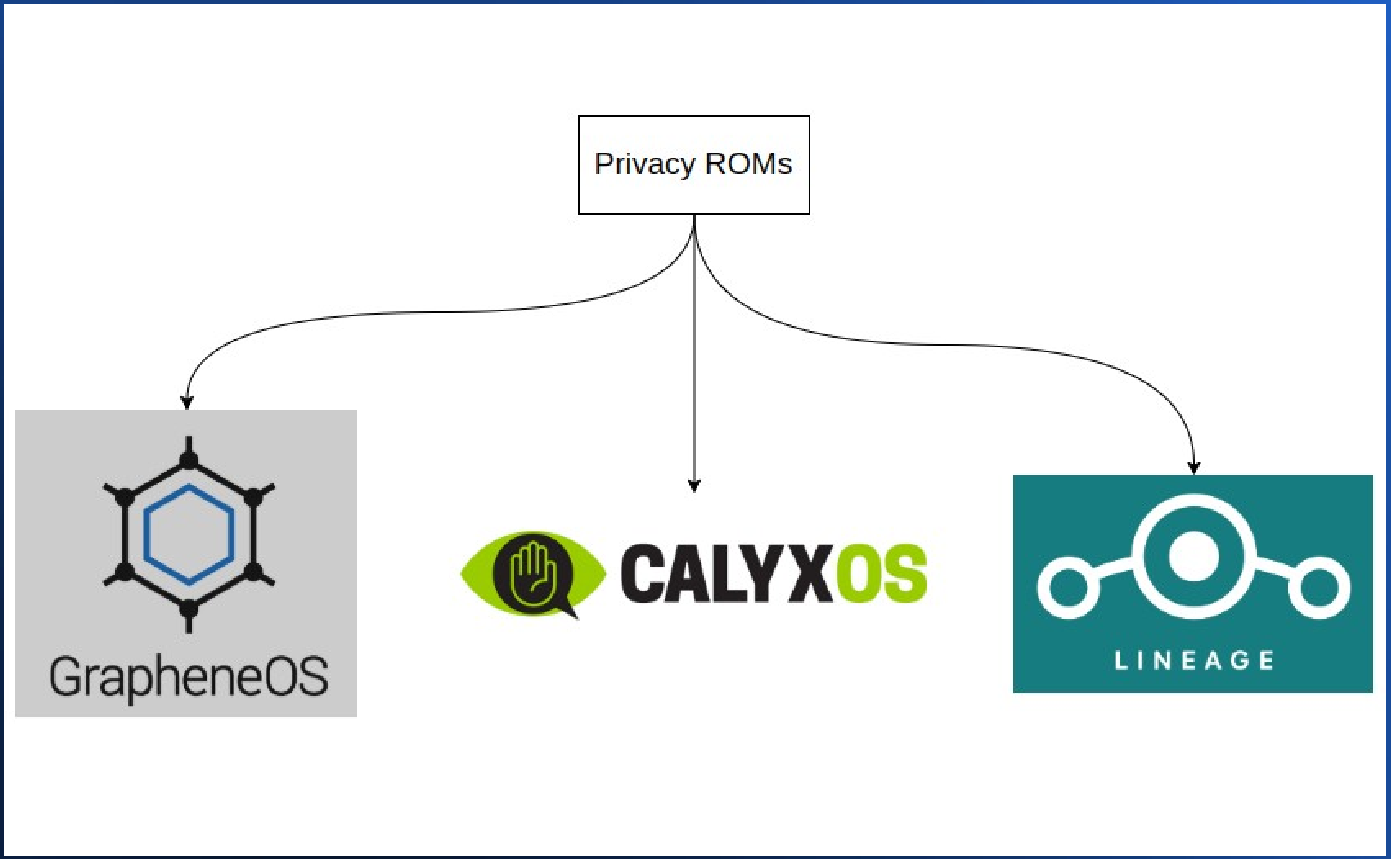
Info

- Find me on Slack/platforms
- Sec eng
- Linux user; recon



"HALF OF LIFE IS FUCKING UP,
THE OTHER HALF IS DEALING WITH IT."
- HENRY ROLLINS

Privacy ROMs



Privacy ROMs

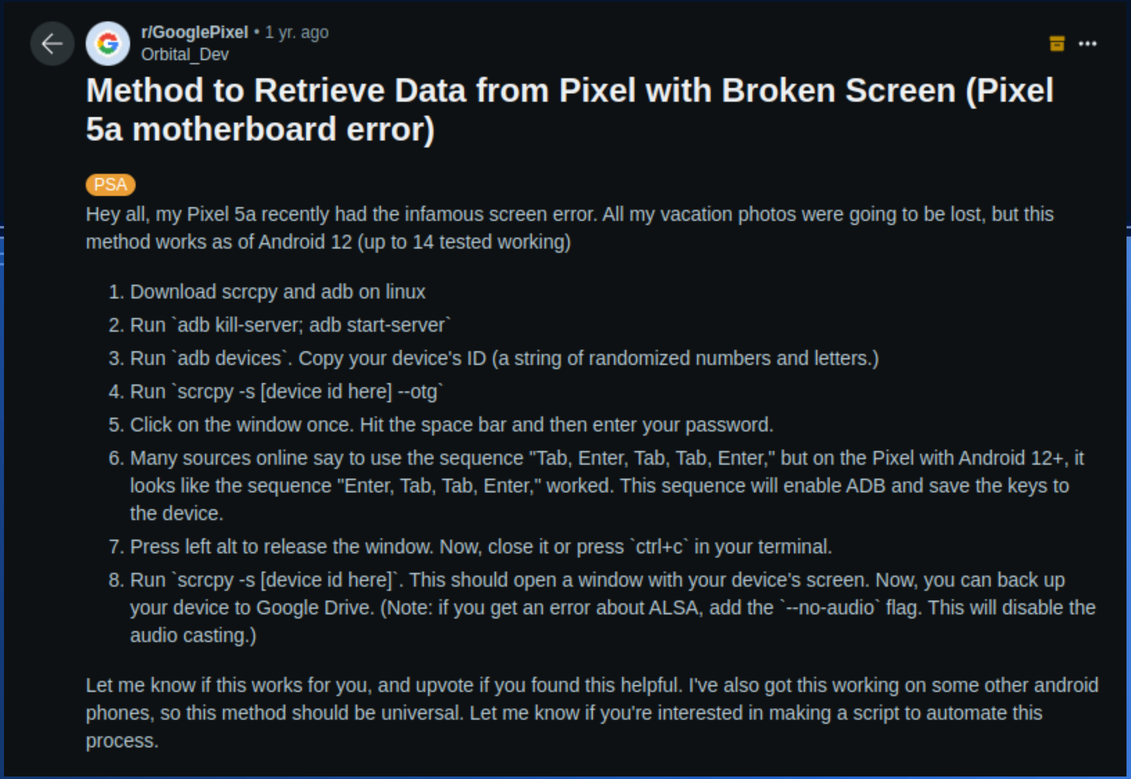
- 3 main ROMs, most support Google Pixels
- Encryption, auto-reboot
- De-googling

My phone

- 01-21 – Phone stops working
- Investigate; QDL Mode
- Try Local Repair Shops, but I know something is wrong
- USB Debugging was already enabled (tap build number in About Phone 9x)
- We can’t scrcpy (screen copy)
- bootloader/firmware corruption :)

The hidden flaw killing Google Pixel phones

Ramblings   November 11, 2022   5 Minutes



r/GooglePixel • 1 yr. ago
Orbital_Dev

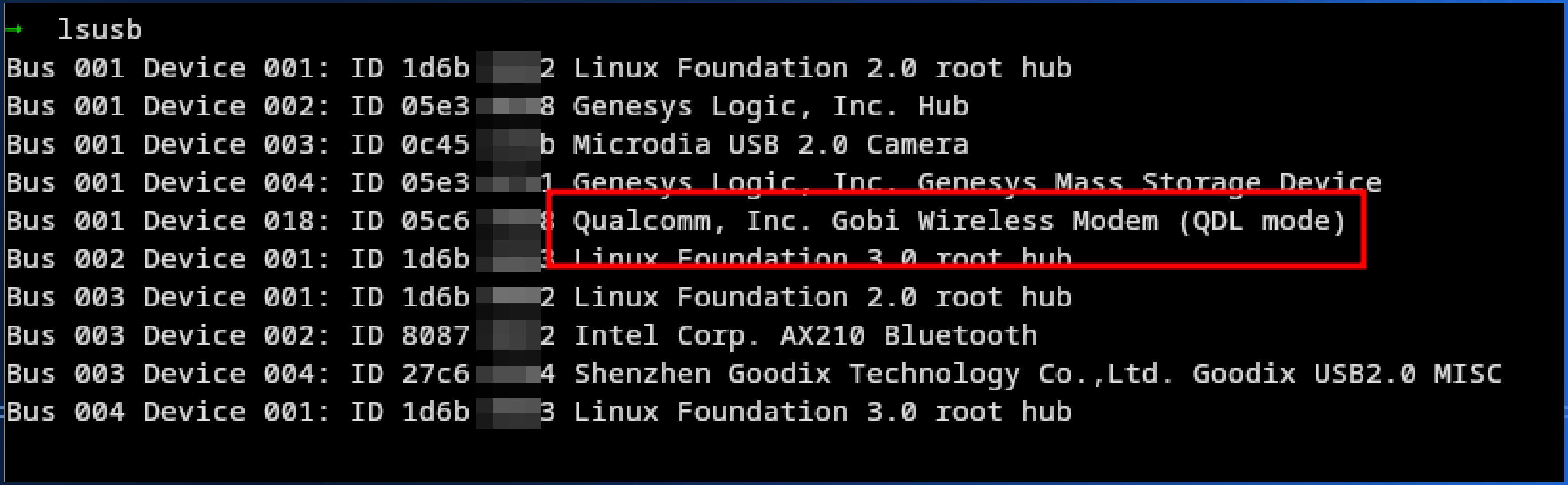
Method to Retrieve Data from Pixel with Broken Screen (Pixel 5a motherboard error)

PSA

Hey all, my Pixel 5a recently had the infamous screen error. All my vacation photos were going to be lost, but this method works as of Android 12 (up to 14 tested working)

1. Download scrcpy and adb on linux
2. Run `adb kill-server; adb start-server`
3. Run `adb devices`. Copy your device's ID (a string of randomized numbers and letters.)
4. Run `scrcpy -s [device id here] --otg`
5. Click on the window once. Hit the space bar and then enter your password.
6. Many sources online say to use the sequence "Tab, Enter, Tab, Tab, Enter," but on the Pixel with Android 12+, it looks like the sequence "Enter, Tab, Tab, Enter," worked. This sequence will enable ADB and save the keys to the device.
7. Press left alt to release the window. Now, close it or press `ctrl+c` in your terminal.
8. Run `scrcpy -s [device id here]`. This should open a window with your device's screen. Now, you can back up your device to Google Drive. (Note: if you get an error about ALSA, add the `--no-audio` flag. This will disable the audio casting.)

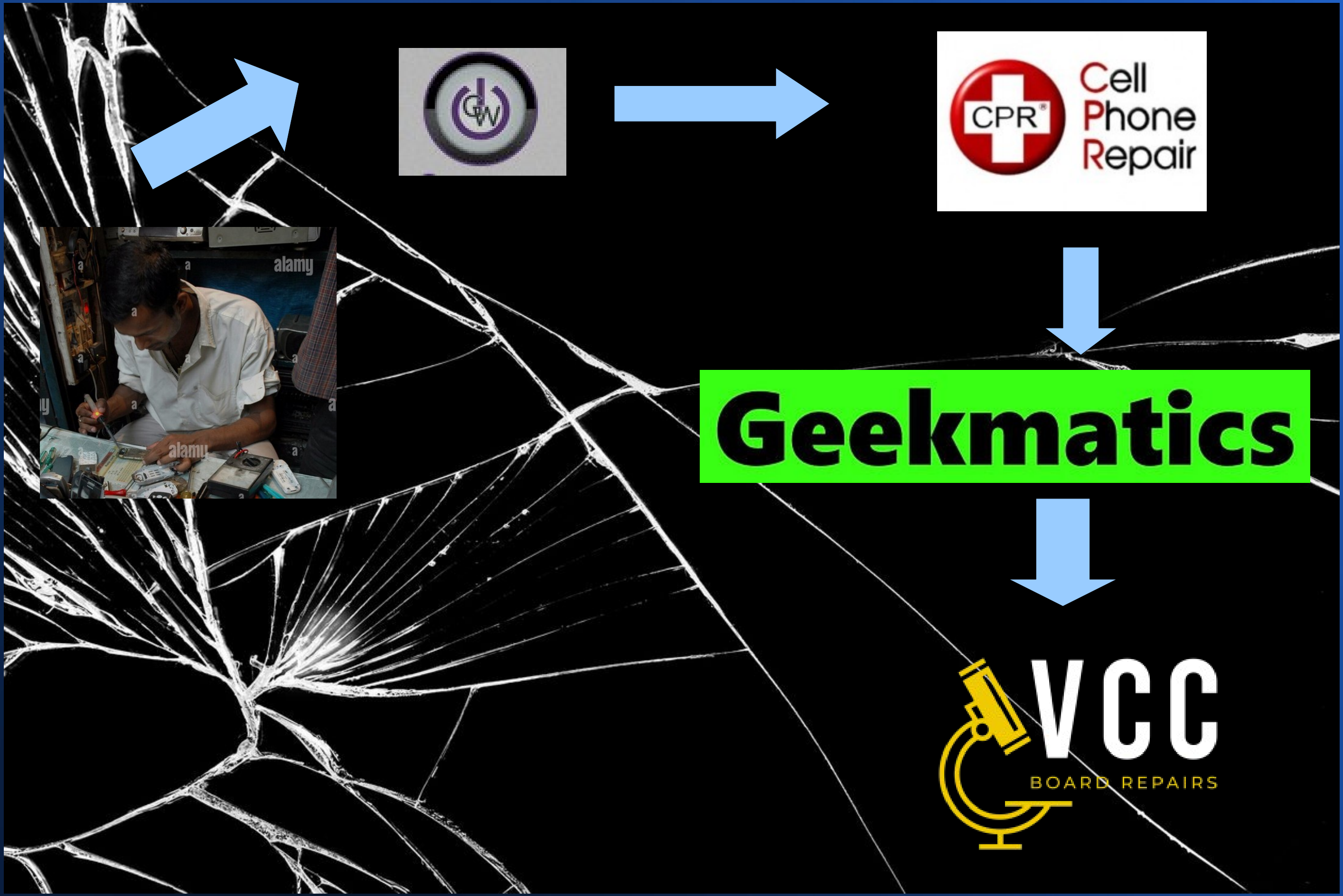
Let me know if this works for you, and upvote if you found this helpful. I've also got this working on some other android phones, so this method should be universal. Let me know if you're interested in making a script to automate this process.



```
→  lsusb
Bus 001 Device 001: ID 1d6b[redacted]2 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 05e3[redacted]8 Genesys Logic, Inc. Hub
Bus 001 Device 003: ID 0c45[redacted]b Microdia USB 2.0 Camera
Bus 001 Device 004: ID 05e3[redacted]1 Genesys Logic, Inc. Genesys Mass Storage Device
Bus 001 Device 018: ID 05c6[redacted]8 Qualcomm, Inc. Gobi Wireless Modem (QDL mode)
Bus 002 Device 001: ID 1d6b[redacted]3 Linux Foundation 3.0 root hub
Bus 003 Device 001: ID 1d6b[redacted]2 Linux Foundation 2.0 root hub
Bus 003 Device 002: ID 8087[redacted]2 Intel Corp. AX210 Bluetooth
Bus 003 Device 004: ID 27c6[redacted]4 Shenzhen Goodix Technology Co.,Ltd. Goodix USB2.0 MISC
Bus 004 Device 001: ID 1d6b[redacted]3 Linux Foundation 3.0 root hub
```

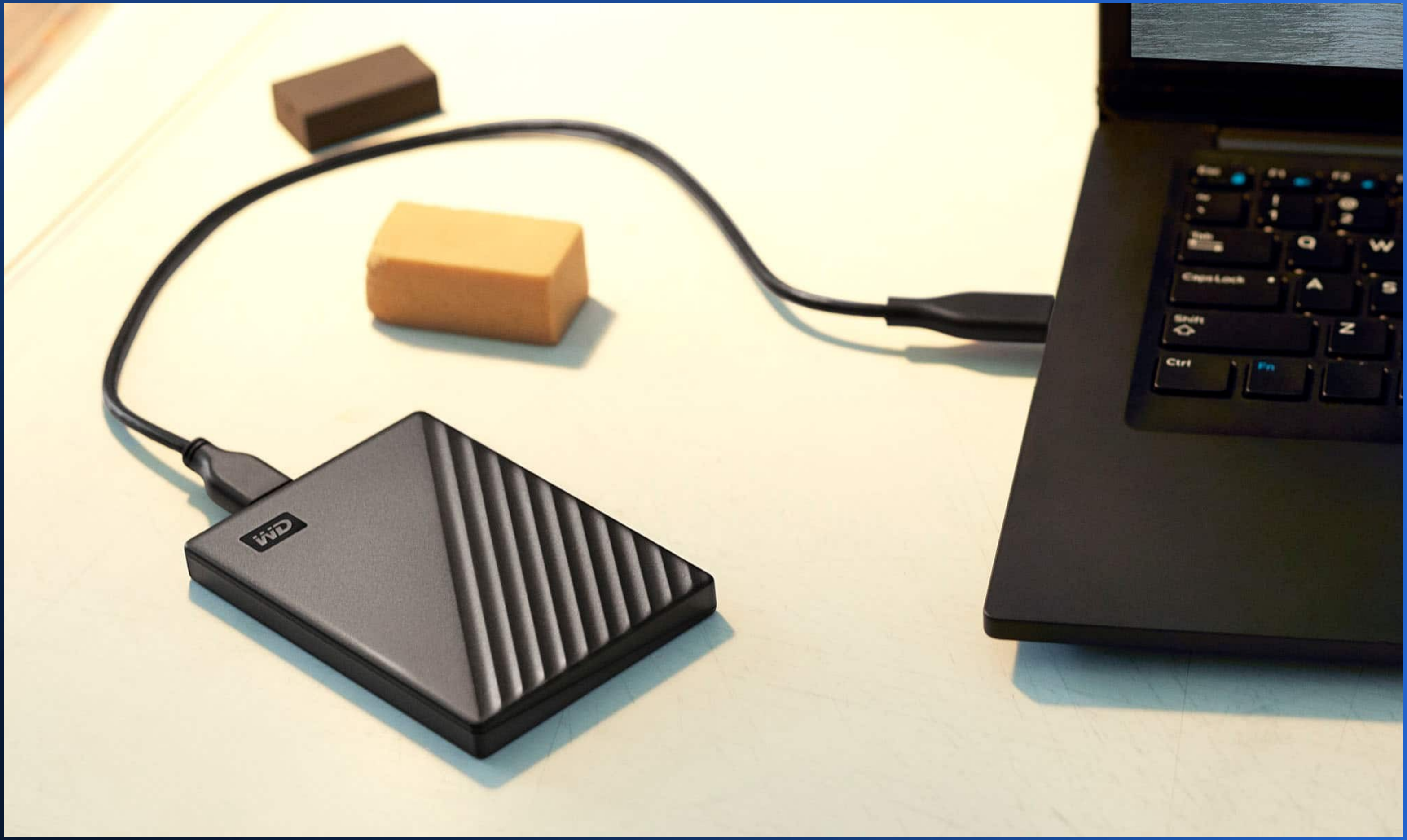
Now What

Phone Repair Journey



- Local Repair shop
- Local Repair Shop x2
- Local Repair Shop x3
- Geekmatics
- VCC Board Repair

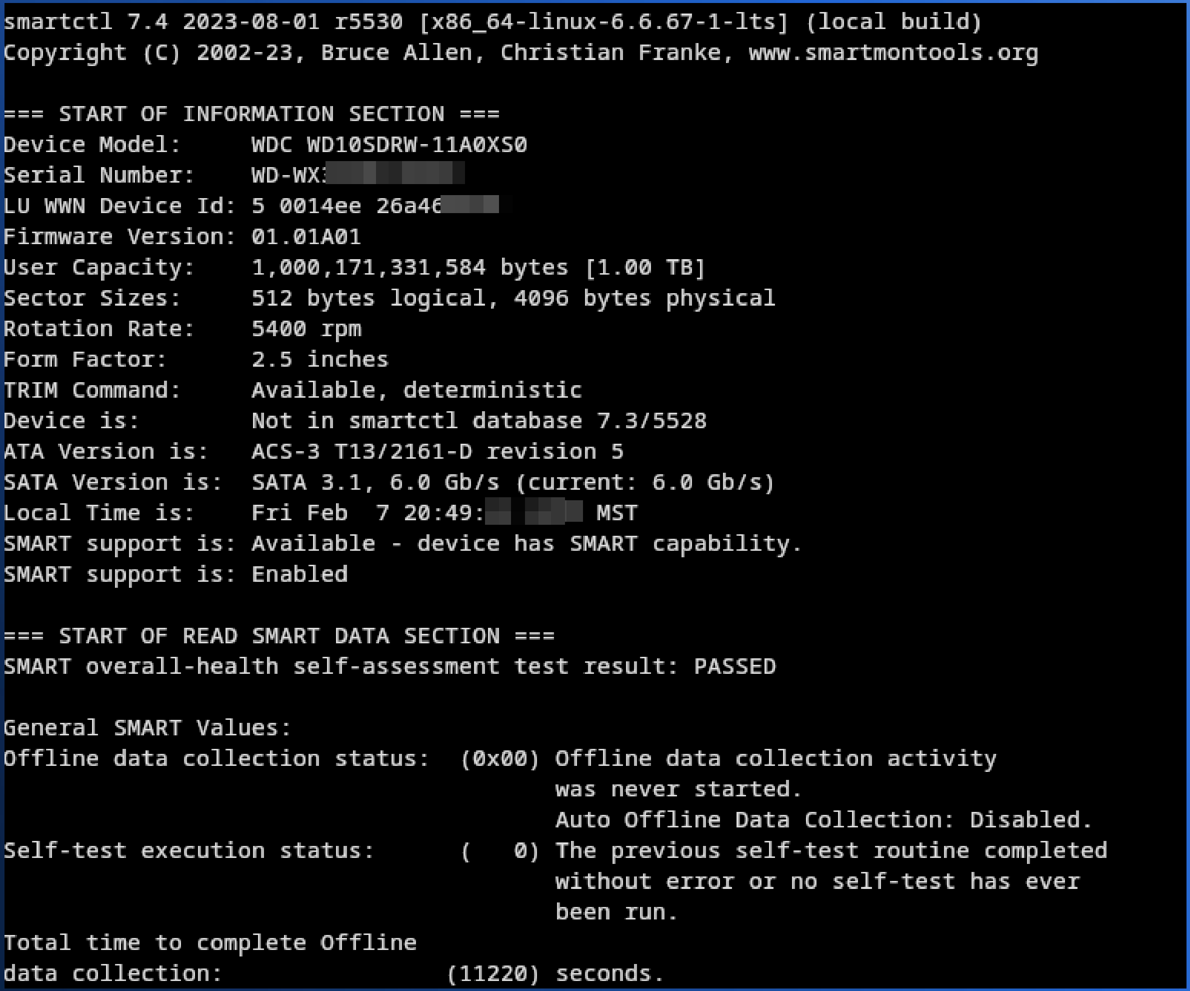
Round 2: Hard Drive Boogaloo



WD Passport

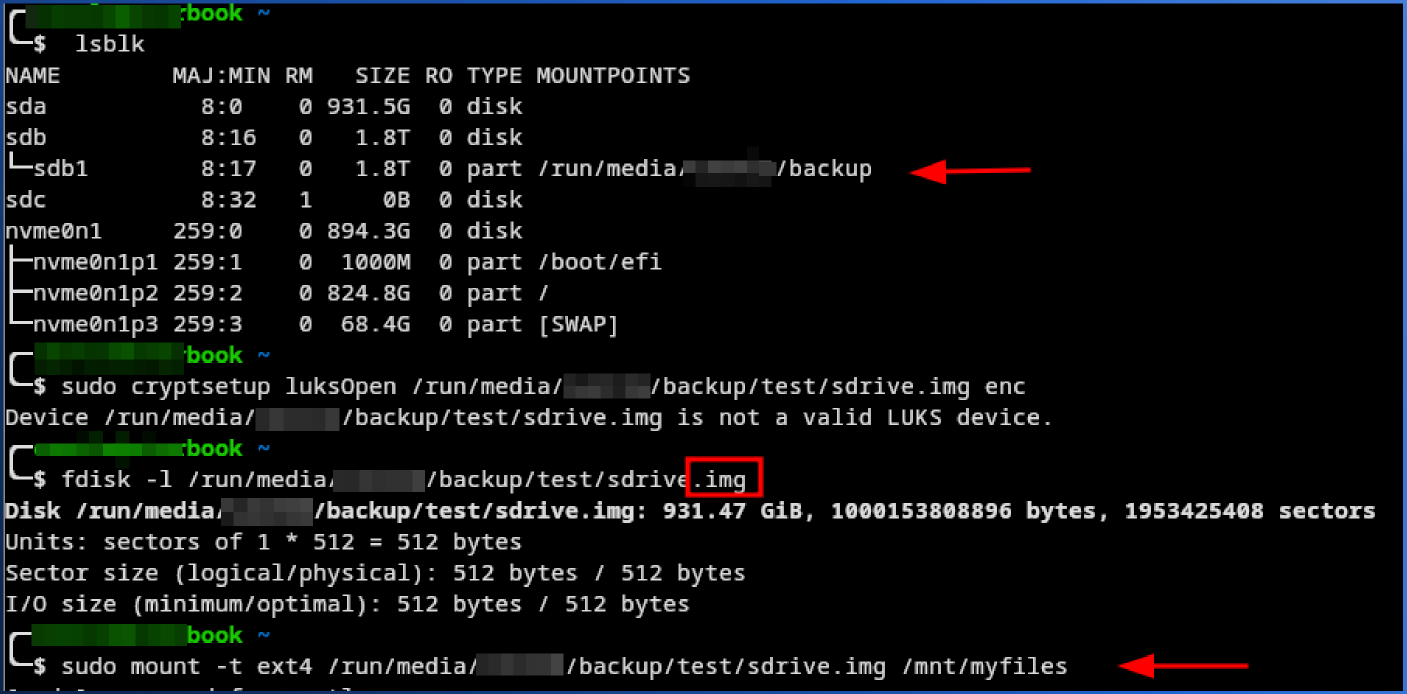
- 02-07 – unrelated to phone, now we have I/O errors on a hard drive with movies/photos
  - No Copy/Paste
  - NO rsync
  - ???
- Standard warranty: 2 years >:)
- Bonus: it’s a LUKS-Encrypted Drive (full drive)

smartctl example

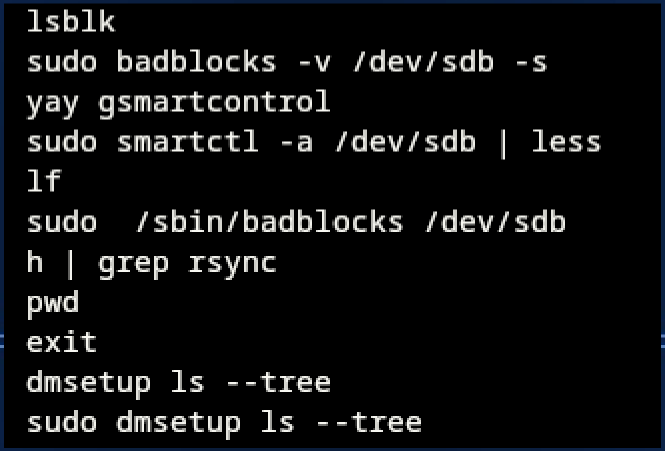


```
smartctl 7.4 2023-08-01 r5530 [x86_64-linux-6.6.67-1-lts] (local build)
Copyright (C) 2002-23, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF INFORMATION SECTION ===
Device Model:     WDC WD10SDRW-11A0XS0
Serial Number:    WD-WX[redacted]
LU WWN Device Id: 5 0014ee 26a46[redacted]
Firmware Version: 01.01A01
User Capacity:    1,000,171,331,584 bytes [1.00 TB]
Sector Sizes:     512 bytes logical, 4096 bytes physical
Rotation Rate:    5400 rpm
Form Factor:      2.5 inches
TRIM Command:     Available, deterministic
Device is:        Not in smartctl database 7.3/5528
ATA Version is:   ACS-3 T13/2161-D revision 5
SATA Version is:  SATA 3.1, 6.0 Gb/s (current: 6.0 Gb/s)
Local Time is:    Fri Feb  7 20:49:[redacted] MST
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

General SMART Values:
Offline data collection status:  (0x00) Offline data collection activity
                                        was never started.
                                        Auto Offline Data Collection: Disabled.
Self-test execution status:      (   0) The previous self-test routine completed
                                        without error or no self-test has ever
                                        been run.
Total time to complete Offline
data collection:                (11220) seconds.
```

I will not be stopped



```
┌[redacted]book ~
└$ lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sda           8:0    0 931.5G  0 disk
sdb           8:16   0   1.8T  0 disk
└─sdb1        8:17   0   1.8T  0 part /run/media/[redacted]/backup
sdc           8:32   1     0B  0 disk
nvme0n1     259:0    0 894.3G  0 disk
├─nvme0n1p1 259:1    0  1000M  0 part /boot/efi
├─nvme0n1p2 259:2    0 824.8G  0 part /
└─nvme0n1p3 259:3    0  68.4G  0 part [SWAP]
┌[redacted]book ~
└$ sudo cryptsetup luksOpen /run/media/[redacted]/backup/test/sdrive.img enc
Device /run/media/[redacted]/backup/test/sdrive.img is not a valid LUKS device.
┌[redacted]book ~
└$ fdisk -l /run/media/[redacted]/backup/test/sdrive.img
Disk /run/media/[redacted]/backup/test/sdrive.img: 931.47 GiB, 1000153808896 bytes, 1953425408 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
┌[redacted]book ~
└$ sudo mount -t ext4 /run/media/[redacted]/backup/test/sdrive.img /mnt/myfiles
```

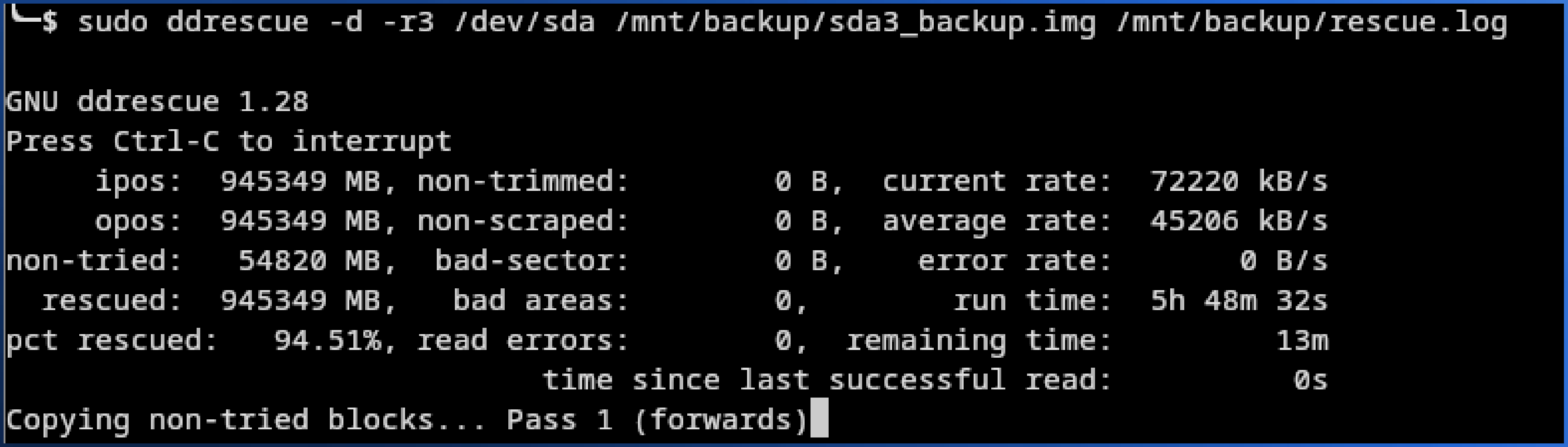


```
lsblk
sudo badblocks -v /dev/sdb -s
yay gsmartcontrol
sudo smartctl -a /dev/sdb | less
lf
sudo  /sbin/badblocks /dev/sdb
h | grep rsync
pwd
exit
dmsetup ls --tree
sudo dmsetup ls --tree
```

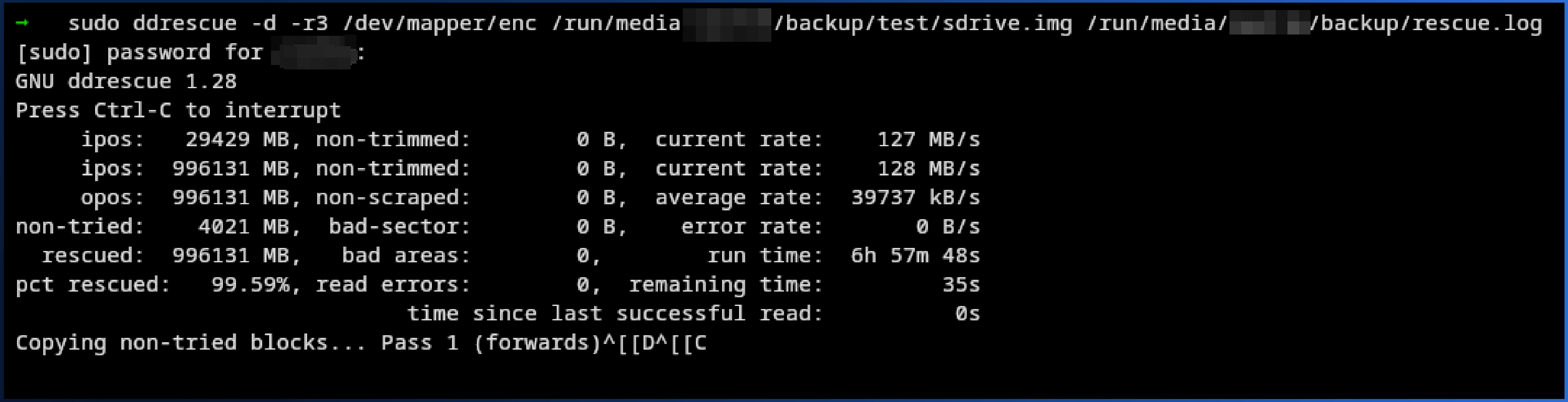
What tools/utilities did we use?

rsync	Synchronization / transfer tool
fdisk	Disk partition/manipulation tool
smartctl	Self-Monitoring, Analysis, Reporting Technology (disc errors)
badblocks	Identify bad sectors
fsck	File system consistency checker/repair. DO NOT MOUNT
photorec/testdisc	Data recovery for lost files/partitions
gnome-disk-utility	GUI disk management for GNOME desktop
losetup	Set up + control loop devices
cryptsetup	Manage LUKS encrypted volumes
dmsetup	Low-level logical volume management
journalctl	Query/display systemd journal logs (svc manager)
dmesg	Display kernel buffer ring messages (search for I/O)
dd	Read/Write/Convert data, or delete by writing on blocks
ddrescue	Data recovery for damaged discs

ddrescue in the end



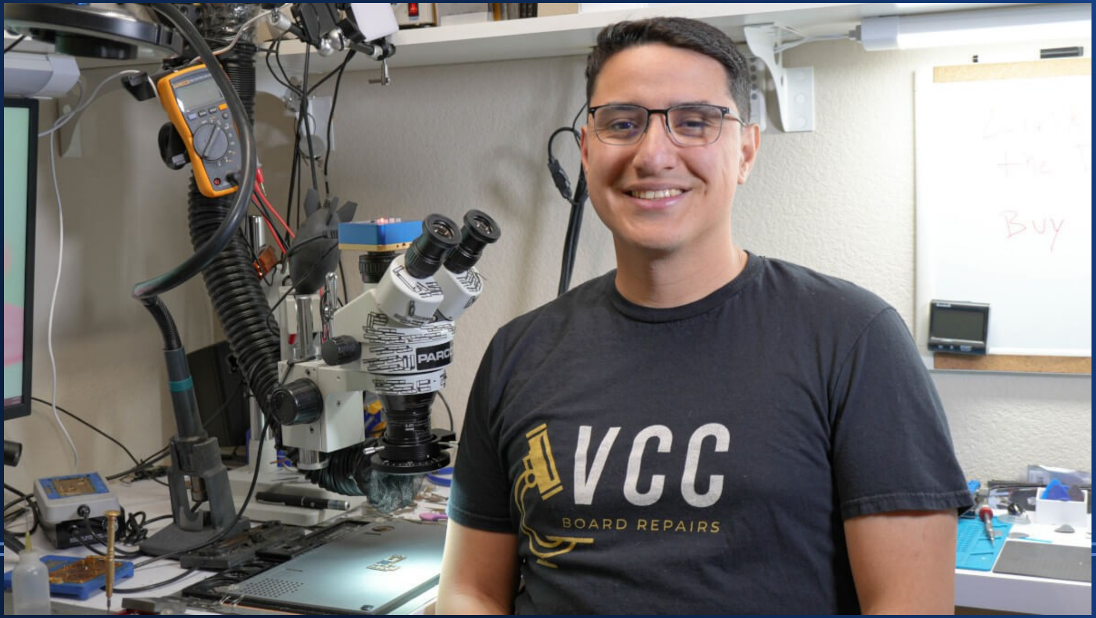
```
└─$ sudo ddrescue -d -r3 /dev/sda /mnt/backup/sda3_backup.img /mnt/backup/rescue.log

GNU ddrescue 1.28
Press Ctrl-C to interrupt
     ipos:  945349 MB, non-trimmed:        0 B,  current rate:  72220 kB/s
     opos:  945349 MB, non-scraped:        0 B,  average rate:  45206 kB/s
non-tried:   54820 MB,  bad-sector:        0 B,    error rate:       0 B/s
  rescued:  945349 MB,   bad areas:        0,        run time:  5h 48m 32s
pct rescued:   94.51%, read errors:        0,  remaining time:        13m
                              time since last successful read:         0s
Copying non-tried blocks... Pass 1 (forwards)
```



```
→  sudo ddrescue -d -r3 /dev/mapper/enc /run/media[redacted]/backup/test/sdrive.img /run/media/[redacted]/backup/rescue.log
[sudo] password for [redacted]:
GNU ddrescue 1.28
Press Ctrl-C to interrupt
     ipos:   29429 MB, non-trimmed:        0 B,  current rate:    127 MB/s
     ipos:  996131 MB, non-trimmed:        0 B,  current rate:    128 MB/s
     opos:  996131 MB, non-scraped:        0 B,  average rate:  39737 kB/s
non-tried:    4021 MB,  bad-sector:        0 B,    error rate:       0 B/s
  rescued:  996131 MB,   bad areas:        0,        run time:  6h 57m 48s
pct rescued:   99.59%, read errors:        0,  remaining time:        35s
                              time since last successful read:         0s
Copying non-tried blocks... Pass 1 (forwards)^[[D^[[C
```

Motherboard Repair

- Jesse Cruz | VCC Board Repairs (Vegas)
- Youtube Channel, dozens of hrs of repair footage
- Open-source (relatively) and self-taught
- UFS + CPU Re-Ball; 2 weeks and $$$



Data Recovery

- STOP using any device you think has issue
- Copy/write-block data if possible
- Leave it to pros
- Back up your stuff, regularly: test backups
- Be persistent, be PATIENT

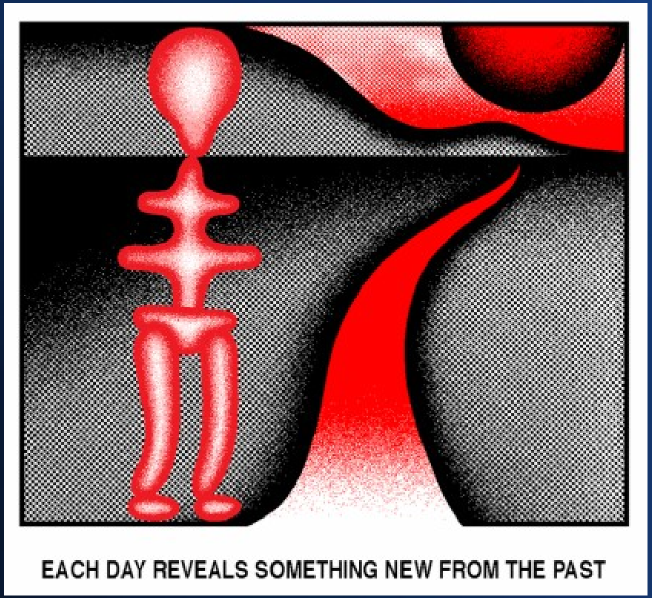
Gillware™

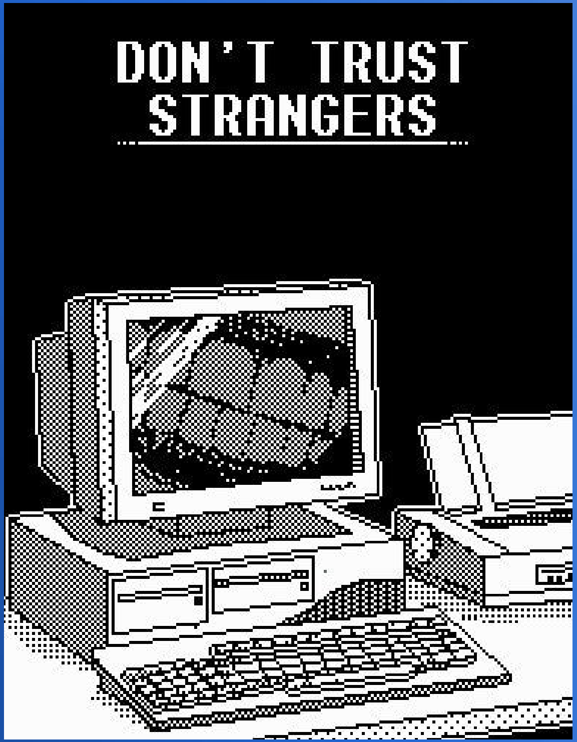
Learning

- Real connections matter
- Phones aren't always important
- People generally want to help
- I went ~2 months without major phone use
- VoIP is useful: independent of SIM
- Can't lose it if it's not on your phone

Future Presentation Ideas

- Overview of Linux Forensics tools
  - data recovery deep dive
- Overview of Privacy-oriented ROMs





Resources

OS
https://grapheneos.org/
https://lineageos.org/
https://calyxos.org/
https://github.com/seedvault-app/seedvault

Misc
https://github.com/Genymobile/scrcpy
https://suspiciouslygeneric.com/2022/11/11/the-hidden-flaw-killing-google-pixel-phones/
https://www.johndstech.com/security/backup-and-mount-disk-images-using-ddrescue/
https://garloff.de/kurt/linux/ddrescue/
https://forensics.wiki/ddrescue/
https://www.baeldung.com/linux/ext4-filesystem-fix-bad-geometry
https://www.youtube.com/c/VCCBoardRepairs/videos
https://vccboardrepairs.com/
https://www.geekmatics.com/
https://www.gillware.com/

+ so many more