Reversing Corruption in Seagate HDD Translators, The Naked Trill Data Recovery Project

By MrDe4d &
Allison Marie Naaktgeboren

Allison Marie Naaktgeboren

- There's more than one Allison Naaktgeboren?!
  - Yes, really. Please yell at the right one
  - 'Naaktgeboren' means 'born naked'"*...may not be obvious at first unless you're Dutch.*" - *PEP20*
- Old Code Monkey
  - Previously at Signal Sciences, Mozilla, FactSet, Amazon, Cisco, RI Biorobotics Laboratory, Coding with Kids
- Community
  - CTF Captain, cofounder QQQa
  - CTF minion, Samurai
  - Algorithms Lead, WWC PDX
  - OWASP Study Night Lead
  - Mentor, PDXWiT & First Robotics
- Carnegie Mellon University, BS in CS
  - "*Differentiable and Piecewise Gaits for Snake Robots*"
  - "*Design of a Modular Snake Robot*"
  - "*Relative Localization in Colony Robots*"

MrDe4d

- Primary researcher; named the project
- Talks at DEF CON, HushCon, Teardown, & Arch Reactor Hackerspace in STL
- Co-founded Revenant Data
- Independent research: SMR technology, AFH manipulation in Seagates,

  MicroJOGs concepts and control
- Self taught except for:
  - Scott Moulton's data recovery training
- BSidesPDX CTF data recovery/forensics challenge with Wireglitch

High Minded Reasons to Care about HDD Repair

- **Right to Know**
  - Lack of standards reduces quality (and costs you money..)
- **Right to Repair**
  - Ownership is not a timeshare! (United States Magnuson-Moss Warranty Act)
- **Right to a less hazardous environment**
  - HDDs aren't compostable, and there are a lot of them
  - Manufacturing materials are bad for humans, bad for the environment

10 secrets the data recovery industry doesn't want you to know (#7 will shock you!)

It’ll Never Happen to Me....

- 50.71% of the HDDs that come through Revenant Data are Seagates
    - 8.16% have some type of translator corruption
- Seagate
    - Started shipping drives in 1980 [Wikipedia]
    - Shipped its 250,000,000th hard drive in 1999[Gnomes, 2000]
    - Shipped F3 architecture, modern translators, 2008
- If 100,000,000 drives active → ~ **8,160,000** cases of translator corruption
- Professional repair can be expensive
    - on the order of ~700-3,000 $ when it happens
    - It is not unheard of for large data recovery companies to charge upward of 8,000 $ for a single case

The Original Quest

- **Seemingly Undamaged HDD & A Really Bad Day™**
- **Corrupted translator suspected**
  - no access to user data or partial access (Spildit, 2013)[6]
  - Is it the **“short points problem”**?
    - Short the read points, gain terminal access, force a regen of translator...**success!**
- **Actually, what other errors can we fix?**
  - Current focus, translators
- **Type of recovery that you can do at home**

Signs Translator may be Corrupted

The hard drive boots[1] but...**ERROR!** **ERROR!** **ERROR!** **ERROR!** **ERROR!**

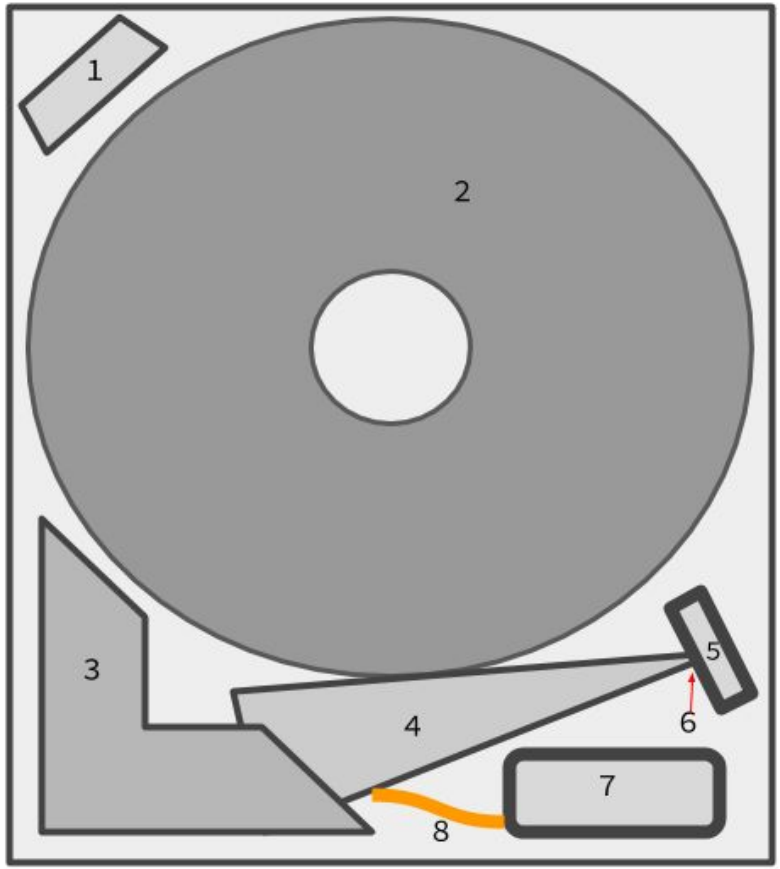
LED: 000000CC FAddr: 0024A051, stuck in busy error

LED:000000CC FAddr:0024A7E5, short the read points[14, 16]

SIM Errors 100*-1008

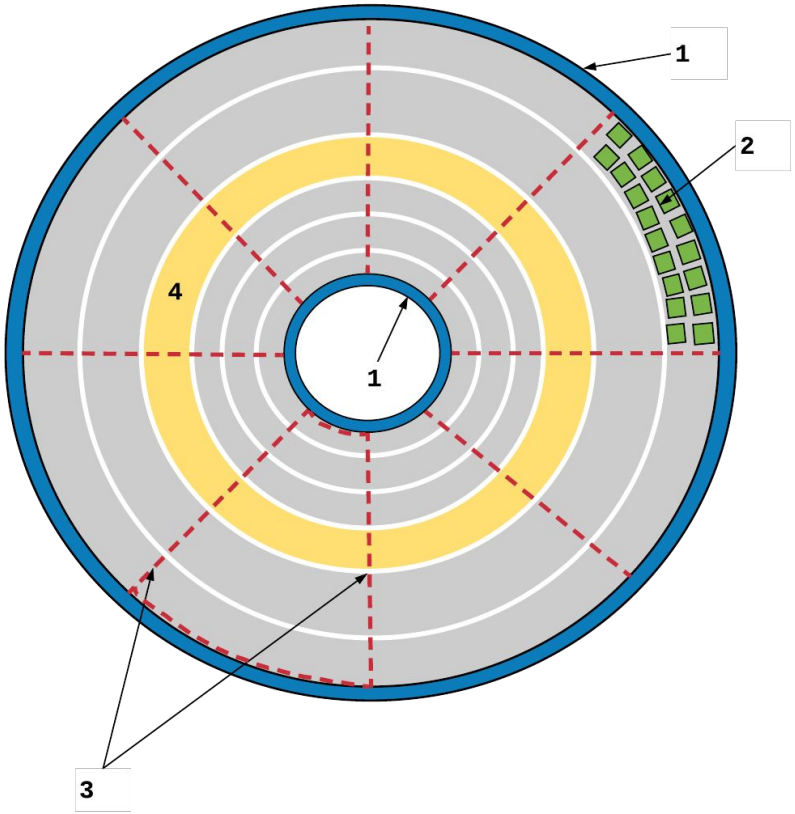
SIM Error 1009

Anatomy of a HDD



1. Filter
2. Platters (aka, the media)
3. Heads magnet, top
4. Actuator arm
5. Heads ramp
6. Heads, outer parked position
7. Head stack connector
8. Connector ribbon

Hard Disk Geometry



1. Service Area
2. Sector
3. Zone
4. Cylinder

Firmware's Usual Suspects

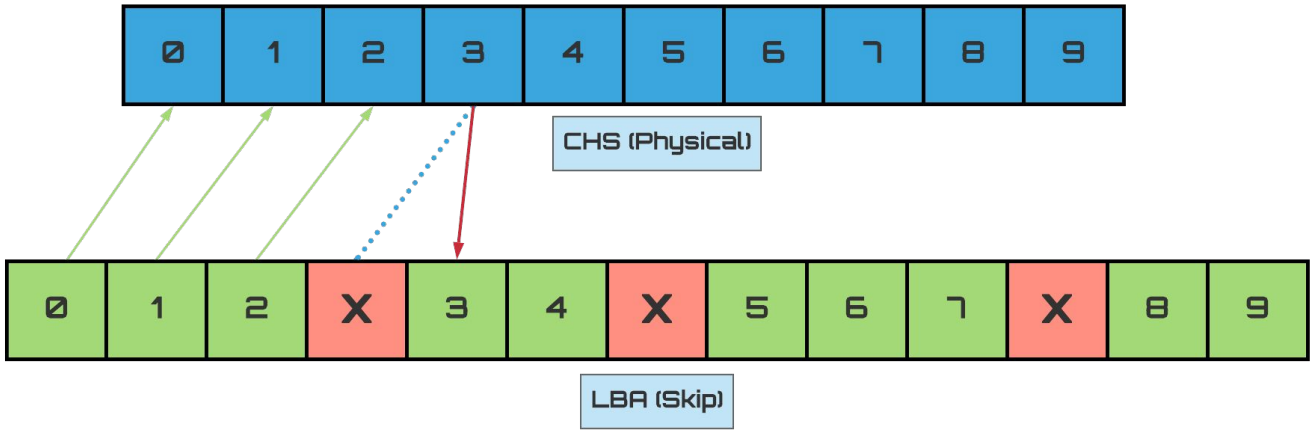
Translator: maps **LBA** (**L**ogical **B**lock **A**ddresses) to **CHS** (**C**ylinder **H**ead **S**ector) & vice versa

- Uses **defect lists** to skip or remap bad sectors
- Without a working translator, HDD can't find the data
- If you wanted to hide some bits from the file system, this isn't a half-bad place to put it[15]

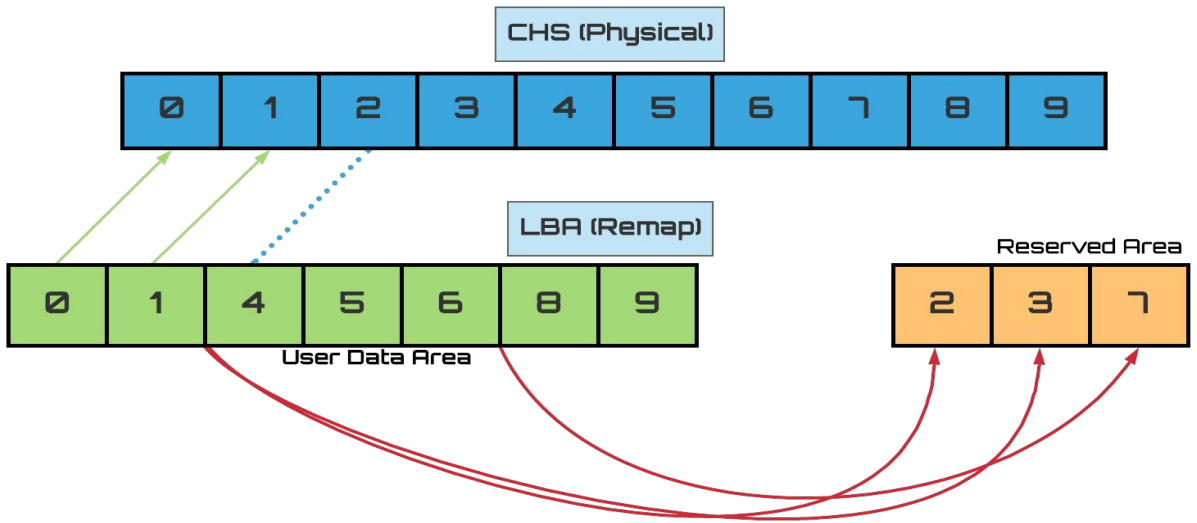
- Primary Defect List
  - Defects found at factory
  - Non-Resident Grown Defect List
    - Second pass for primary defects performed at factory (Seagate-specific)
- Grown Defect List
  - Defects accumulated over time
  - Potentially ~2GB of "spare" space/sectors exists in the the G-List

There are others: overlays, head adaptives, SMART etc, that are not relevant to this talk

Physical to Logical (skip)



Physical to Logical (remap)



Our Foolproof Plan Cannot Possibly Fail

1. Controlled corruption of a translator on a target drive
    a. finite space is allocated for g-list, overfill it!
2. Run through a manual fix
3. Model it with a program
4. Test it on unsuspecting members of hackerspace
5. ???
6. Profit!

If we knew what we were doing, it wouldn't be called research...

Translator Defect Lists: Primary

Seagate Name	Type	Class	Attributes
Primary Defect List (P-List)	Fixed	Skip	> Factory defects found after initial Self Scan Test > Used to generate the translator
Non-Resident Defect List (NRG-List)	Fixed	Skip	> Factory defects found after *second* Self Scan Test > Often empty > May act as reserved space

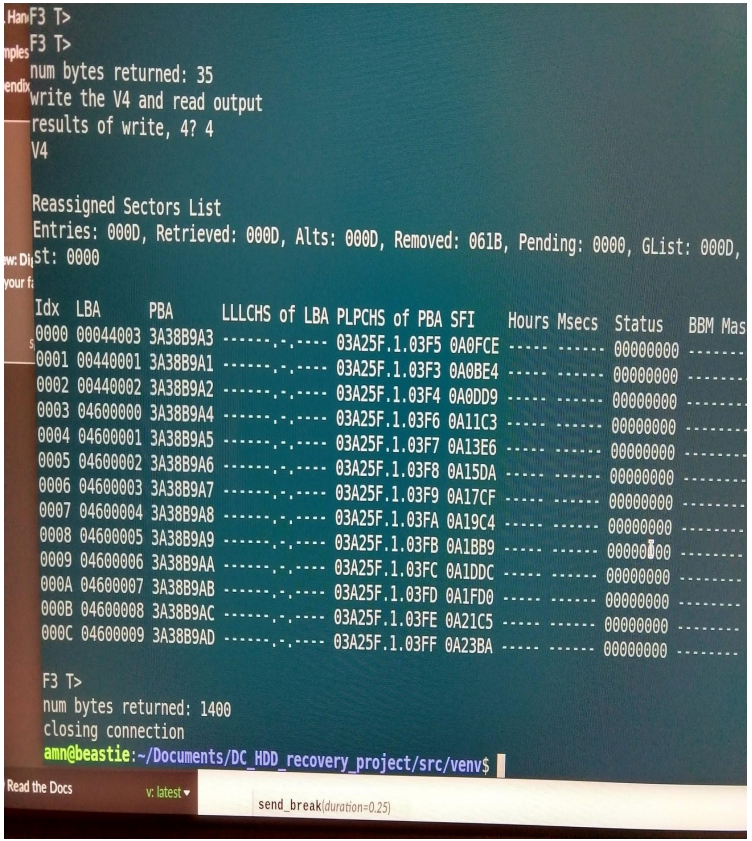
Translator Defect Lists: Grown

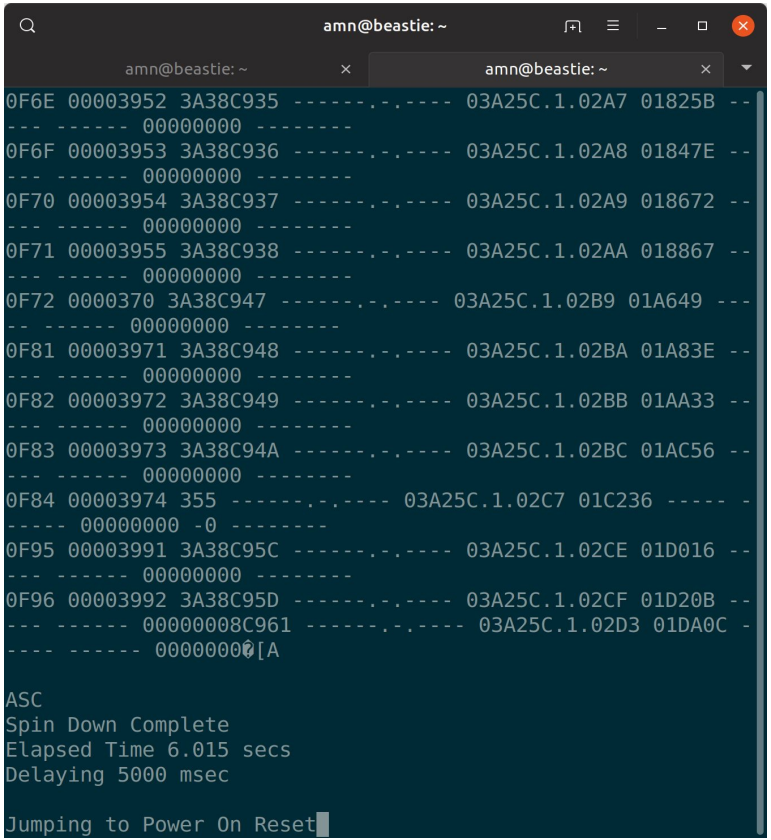
Seagate Name	Type	Class	Attributes
Grown Defect List (G-List)	Dynamic	Remap	> Cumulative, reallocated bad blocks > "Copied" sectors > "Synced" with the Alt-List
Alternate Defect List (Alt-List)	Dynamic	Remap	> Cumulative, pending bad blocks > Occur during read operation only > "Synced" with G-List
Track Defect List (T-List)	Dynamic?	Remap?	> Output similar to Alt-List > Records of entries (by geometry) > P-List & NRG-List combination?

Translator Lists: SLIP-Lists

Seagate Name	Type	Class	Attributes
User Slip Defect List (USDL)	Fixed?	Skip?	> Combination of P-List & NRG-List > Result of data wedge-wise asynchronous disk rotation [7]
SLIP List & System Slip Defect List (SSDL)	Dynamic?	Unknown	> SA Defects List > *Or* suspected records of protocol errors/defects between HDD and host

Sanity Checking-- LHS: Script RHS: Screen

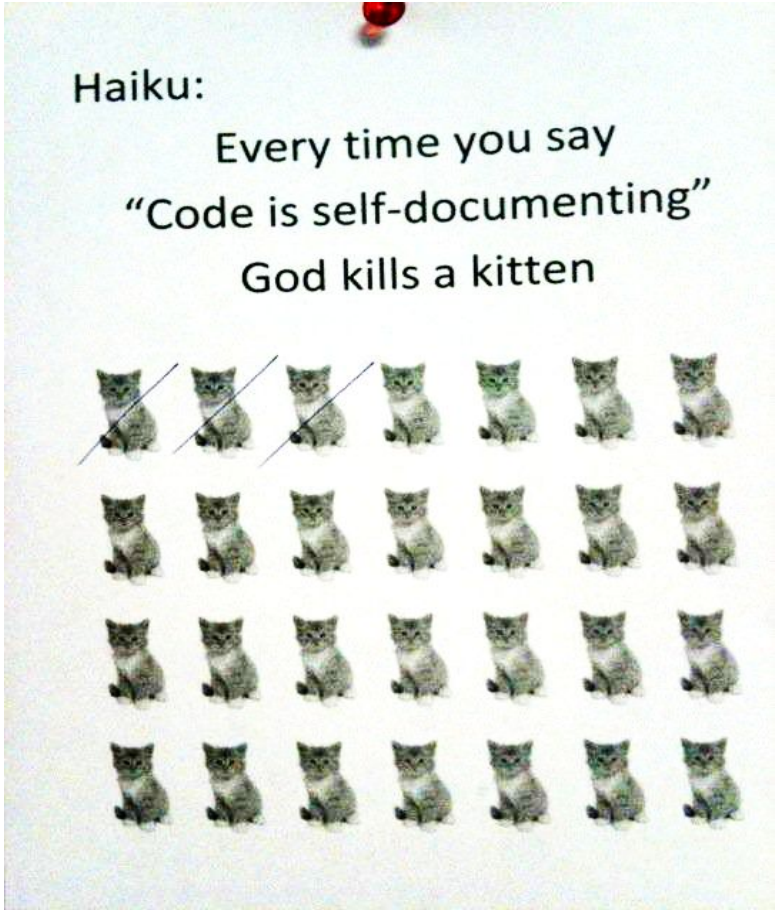




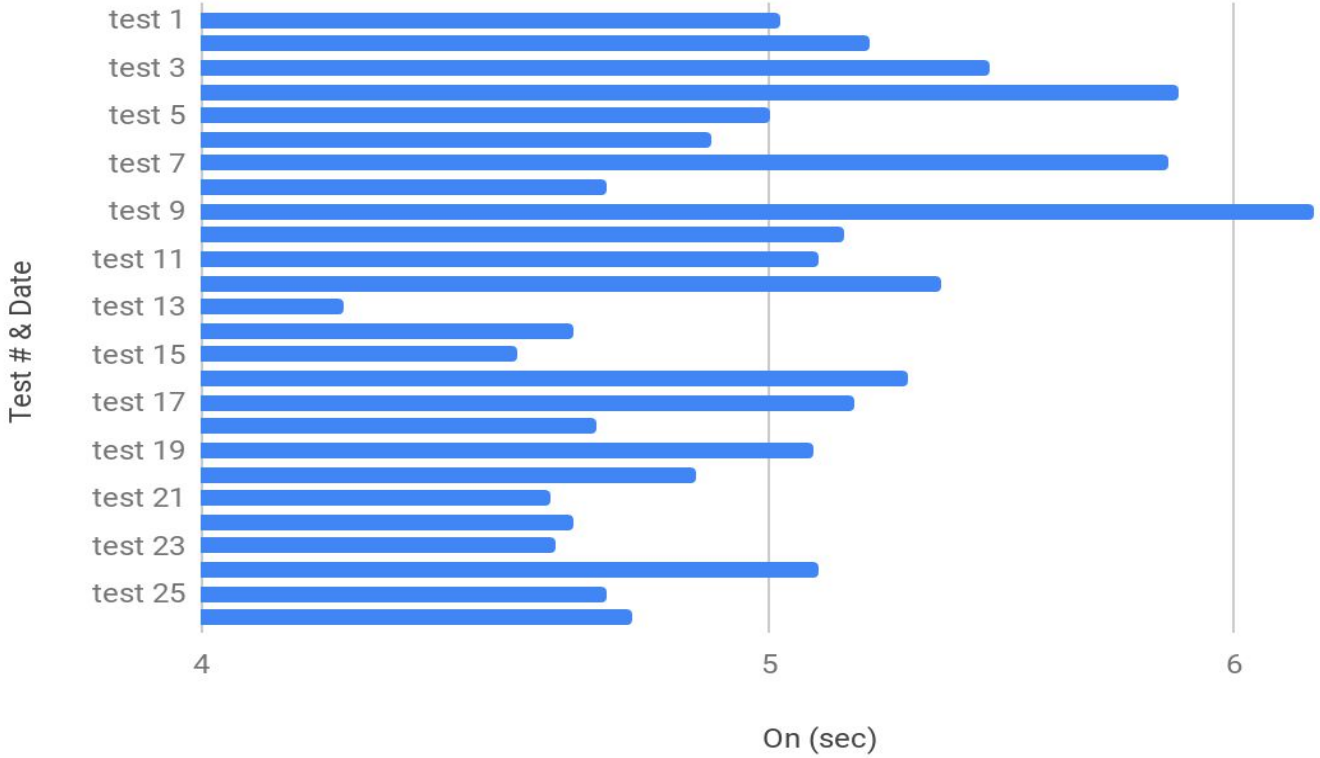
Firmware is Weird

Quick! What do these do?

- `F3 6> E2`
- `F3 T> i4,1,22`



A Window Both Narrow and Wide



The (mis)Adventure So Far...

Surprises

- There were more lists in firmware than anticipated
  - which one(s) should we target?
- Differences in firmware behavior between versions
  - AP63 vs CC38 vs CC45 vs JC4A
- Translator proved smarter than anticipated
- G-List has more space than anticipated
- Firmware code is really difficult to grok

Hurdles

- Problems between seat & workbench
  - Human errors
    - Software engineer can't hardware
    - Hardware engineer can't software
- Significant Timing Variance
  - Cmd output could take ~1 sec to 6 min
- Pyserial was less reliable than anticipated
  - PySerial on Windows not recommended

Where we are now..

- We can reverse corruption if the diagnostic mode is available
  - Ex **SIM Error 1009**
- We can consistently corrupt the target drives
- But…. we haven’t yet been able to reproduce the original target solution under observation

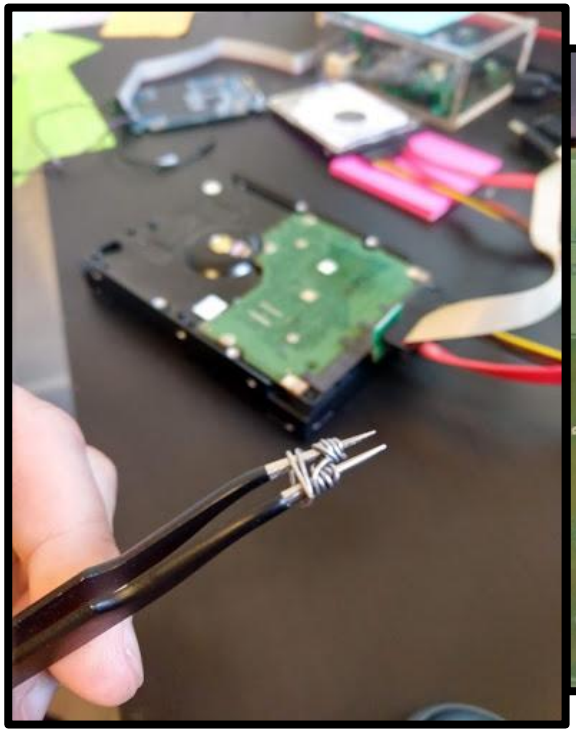
WIP++

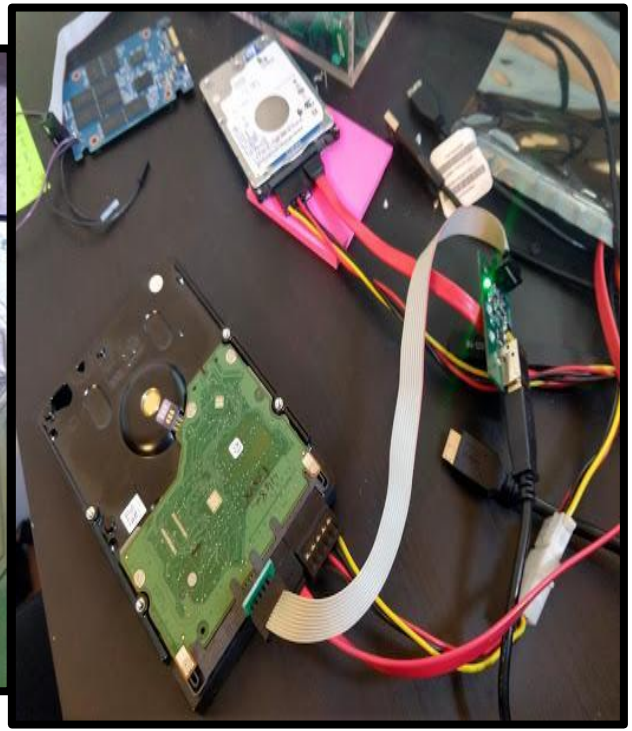
- Not all hackers are coders and not all coders are hackers
  - Exclusion of non-coders makes my hacker spirit sad
- Written to help those that don’t code understand
  - Code deliberately simplistic and procedural
  - I’d like to enable everyone to learn
- Python is the lingua franca of security, C is very useful
- GPL v3 : Sharing is Caring

What You'll Need to DIY

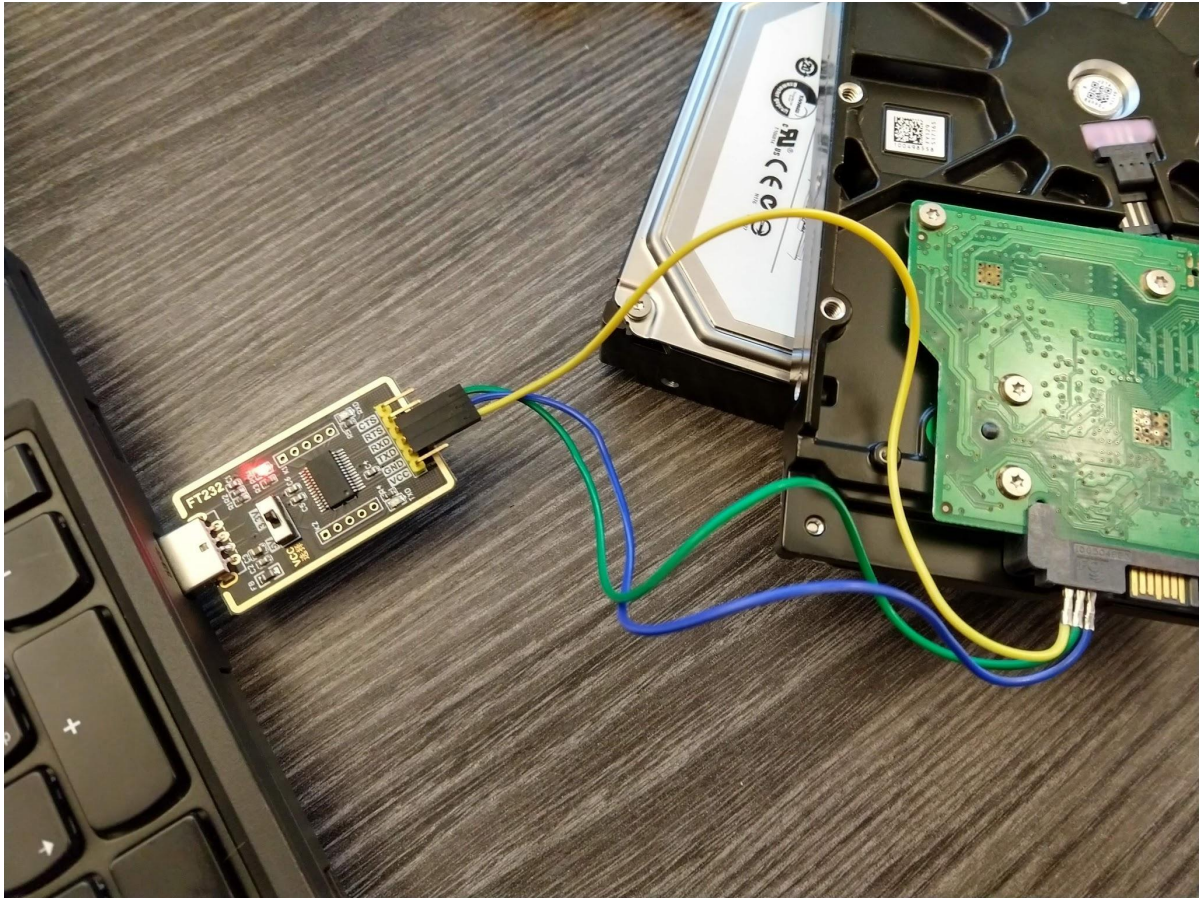
- USB to TTL Adapter with a FTDI Chip FT232RL ($3-$15)
- Access to the TX RX & GND pins
- Power adapter (or TTL with shared-host power)
- Code
  - https://github.com/anaaktge/naked-trill-hdd-recovery
  - PySerial module
- **[ENCOURAGED]** install Screen
- **[STRONGLY ENCOURAGED]**
  - Test hard drives identical to the "patient"
    - Match the model number
    - Drive family of Pharaoh, Moose (ID via debug mode, model# OK)
    - Firmware versions
      - This type of corruption may **not** occur in Dell specific fw version JC4A
      - Apple fw has its own set of rules too

Our Setup





Connection Layout



Pin Set-Up

- RX on TTL matches the TX on the HDD
- GND is 3rd to the left from SATA with PCB facing up
- [power connector not shown]

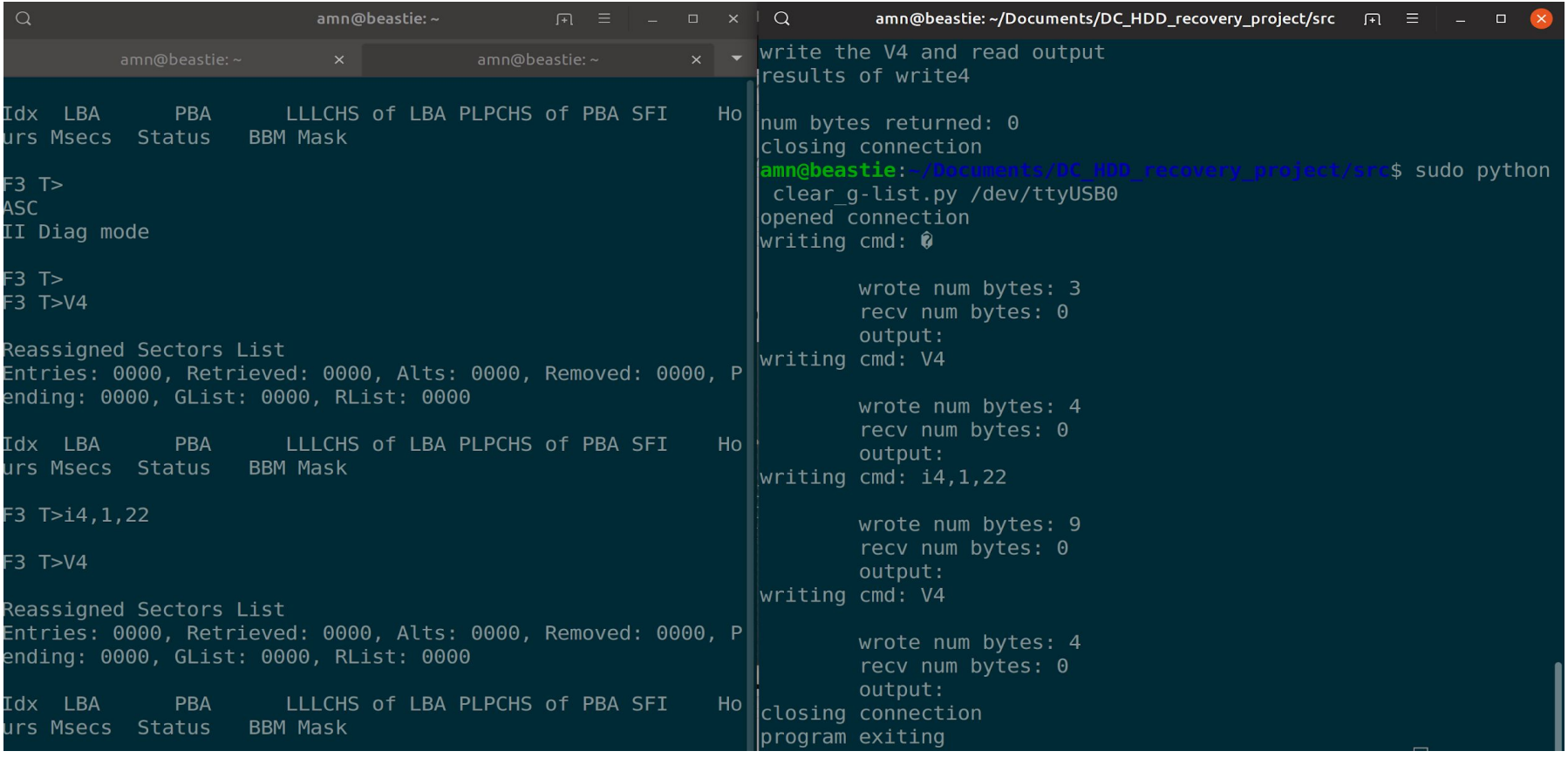
Please Be Very Careful!

Not everything done in firmware can be undone.

You Got This!

1. Get software installed and in order
    - chmod is your friend
2. Hook up connectors
    - double check your connectors
3. Determine what port your os assigned
    - ex) COM1 on windows, ttyusb0 on linux
    - linux:
        - we used dmesg to check
        - Screen to vet a manual connection
4. Run scripts with required arguments in specified order. RTFM.

Like a G(list) Six



What's Next?

Continued Work

- Solve the original problem without shorting if possible
- Configure translator rebuild based on lists you specify
- Expand to include other Seagate families and HDD manufacturers
    - Implement via ATA commands

Help Wanted

- Long term goal: open source data recovery suite
- Feature requests
- Code & documentation contributions
- Help testing
- Open knowledge about the firmware

Acknowledgements & Thanks

- Justin Hibbits (firmware),
- Wireglitch (data recovery),
- Mawlee (social engineer for pricing),
- Fraser Corrance (data recovery expert),
- Fzabkar (data recovery researcher),
- Spritesmods aka Jeroen Domburg (firmware researcher, prior research),
- Spildit (data recovery researcher, HDDOracle founder),
- Securelyfitz & px (cfp feedback)

Bibliography

https://github.com/ActualMrDe4d/Naked-Trill-Data-Recovery-Project/blob/master/README.md

OR: **kik.to/y7**

repo:

https://github.com/anaaktge/naked-trill-hdd-recovery