

# 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..)

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

- **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

# 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<sup>1</sup> but...**ERROR!**      **ERROR!**      **ERROR!**      **ERROR!**      **ERROR!**

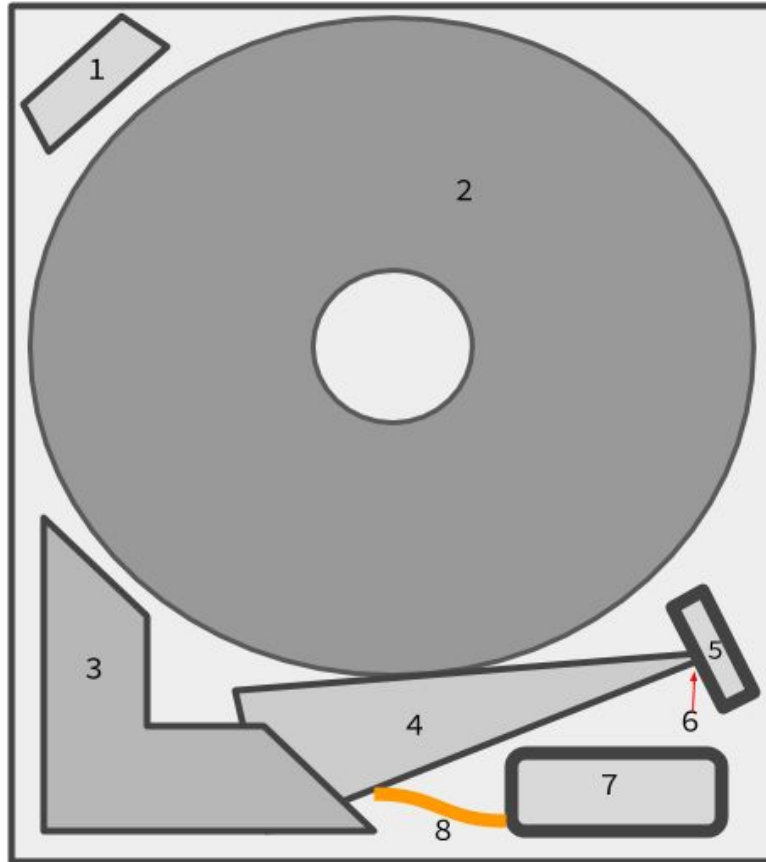
LED: 000000CC FAddr: 0024A051, stuck in busy error

LED:000000CC FAddr:0024A7E5, short the read points<sup>14, 16</sup>

SIM Errors 100\*-1008

SIM Error 1009

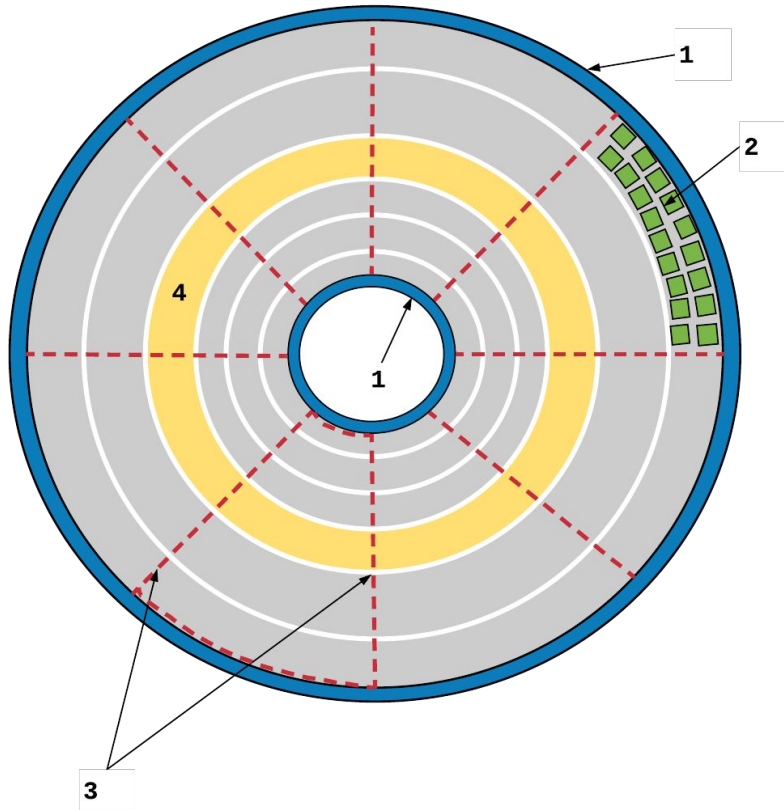
# Anatomy of a HDD



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

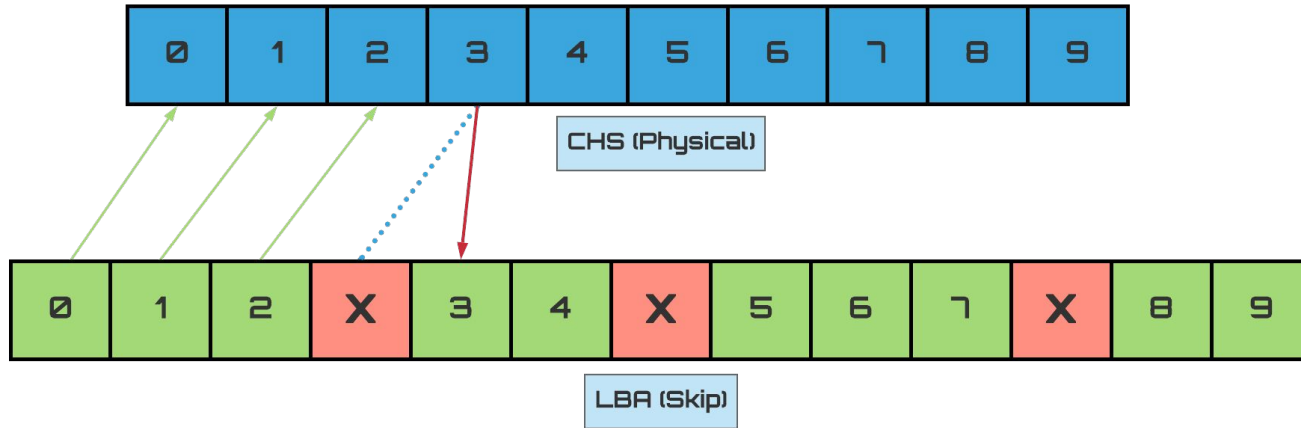
**Translator:** maps **LBA** (Logical **B**lock **A**ddresses) to **CHS** (Cylinder **H**ead **S**ector) & vice versa

- 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<sup>15</sup>

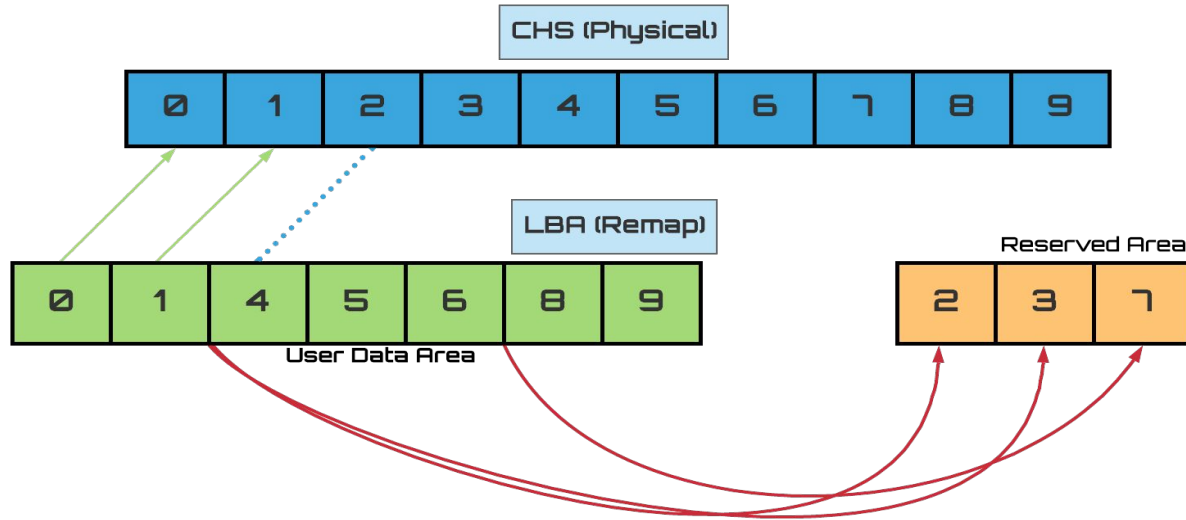
- Primary Defect List
  - Defects found at factory
  - Non-Resident Grown Defect List
    - Second pass for primary defects performed at factory (Seagate-specific)
- Grown Defect List
  - Defects accumulated over time
  - Potentially ~2GB of “spare” space/sectors exists in the the G-List

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	<ul style="list-style-type: none"><li>&gt; Factory defects found after initial Self Scan Test<ul style="list-style-type: none"><li>&gt; Used to generate the translator</li></ul></li></ul>
Non-Resident Defect List (NRG-List)	Fixed	Skip	<ul style="list-style-type: none"><li>&gt; Factory defects found after <i>second</i> Self Scan Test<ul style="list-style-type: none"><li>&gt; Often empty</li><li>&gt; May act as reserved space</li></ul></li></ul>

## Translator Defect Lists: Grown

Seagate Name	Type	Class	Attributes
Grown Defect List (G-List)	Dynamic	Remap	<ul style="list-style-type: none"><li>&gt; Cumulative, reallocated bad blocks<ul style="list-style-type: none"><li>&gt; "Copied" sectors</li><li>&gt; "Synced" with the Alt-List</li></ul></li></ul>
Alternate Defect List (Alt-List)	Dynamic	Remap	<ul style="list-style-type: none"><li>&gt; Cumulative, pending bad blocks<ul style="list-style-type: none"><li>&gt; Occur during read operation only</li><li>&gt; "Synced" with G-List</li></ul></li></ul>
Track Defect List (T-List)	Dynamic?	Remap?	<ul style="list-style-type: none"><li>&gt; Output similar to Alt-List<ul style="list-style-type: none"><li>&gt; Records of entries (by geometry)</li><li>&gt; P-List &amp; NRG-List combination?</li></ul></li></ul>



## Translator Lists: SLIP-Lists

Seagate Name	Type	Class	Attributes
User Slip Defect List (USDL)	Fixed?	Skip?	<ul style="list-style-type: none"><li>&gt; Combination of P-List &amp; NRG-List</li><li>&gt; Result of data wedge-wise asynchronous disk rotation [7]</li></ul>
SLIP List & System Slip Defect List (SSDL)	Dynamic?	Unknown	<ul style="list-style-type: none"><li>&gt; SA Defects List</li><li>&gt; Or suspected records of protocol errors/defects between HDD and host</li></ul>

# Sanity Checking-- LHS: Script RHS: Screen

```
ManF3 T>
F3 T>
num bytes returned: 35
write the V4 and read output
results of write, 4? 4
V4

Reassigned Sectors List
Entries: 000D, Retrieved: 000D, Alts: 000D, Removed: 061B, Pending: 0000, GList: 000D,
st: 0000

Idx LBA PBA LLLCHS of LBA PLPCHS of PBA SFI Hours Msecs Status BBM Mas
0000 00044003 3A38B9A3 -----,----- 03A25F.1.03F5 0A0FCE ----- 00000000 -----
0001 00440001 3A38B9A1 -----,----- 03A25F.1.03F3 0A0BE4 ----- 00000000 -----
0002 00440002 3A38B9A2 -----,----- 03A25F.1.03F4 0A0DD9 ----- 00000000 -----
0003 04600000 3A38B9A4 -----,----- 03A25F.1.03F6 0A11C3 ----- 00000000 -----
0004 04600001 3A38B9A5 -----,----- 03A25F.1.03F7 0A13E6 ----- 00000000 -----
0005 04600002 3A38B9A6 -----,----- 03A25F.1.03F8 0A15DA ----- 00000000 -----
0006 04600003 3A38B9A7 -----,----- 03A25F.1.03F9 0A17CF ----- 00000000 -----
0007 04600004 3A38B9A8 -----,----- 03A25F.1.03FA 0A19C4 ----- 00000000 -----
0008 04600005 3A38B9A9 -----,----- 03A25F.1.03FB 0A1BB9 ----- 00000000 -----
0009 04600006 3A38B9AA -----,----- 03A25F.1.03FC 0A1DDC ----- 00000000 -----
000A 04600007 3A38B9AB -----,----- 03A25F.1.03FD 0A1FD0 ----- 00000000 -----
000B 04600008 3A38B9AC -----,----- 03A25F.1.03FE 0A21C5 ----- 00000000 -----
000C 04600009 3A38B9AD -----,----- 03A25F.1.03FF 0A23BA ----- 00000000 -----

F3 T>
num bytes returned: 1400
closing connection
amn@beastie:~/Documents/DC_HDD_recovery_project/src/venv$
```

```
amn@beastie: ~
amn@beastie: ~ x amn@beastie: ~ x
0F6E 00003952 3A38C935 -----,----- 03A25C.1.02A7 01825B --
--- 00000000 -----
0F6F 00003953 3A38C936 -----,----- 03A25C.1.02A8 01847E --
--- 00000000 -----
0F70 00003954 3A38C937 -----,----- 03A25C.1.02A9 018672 --
--- 00000000 -----
0F71 00003955 3A38C938 -----,----- 03A25C.1.02AA 018867 --
--- 00000000 -----
0F72 00003970 3A38C947 -----,----- 03A25C.1.02B9 01A649 --
--- 00000000 -----
0F81 00003971 3A38C948 -----,----- 03A25C.1.02BA 01A83E --
--- 00000000 -----
0F82 00003972 3A38C949 -----,----- 03A25C.1.02BB 01AA33 --
--- 00000000 -----
0F83 00003973 3A38C94A -----,----- 03A25C.1.02BC 01AC56 --
--- 00000000 -----
0F84 00003974 355 -----,----- 03A25C.1.02C7 01C236 -----
--- 00000000 -0 -----
0F95 00003991 3A38C95C -----,----- 03A25C.1.02CE 01D016 --
--- 00000000 -----
0F96 00003992 3A38C95D -----,----- 03A25C.1.02CF 01D20B --
--- 00000008C961 ----- 03A25C.1.02D3 01DA0C --
--- 00000000[A

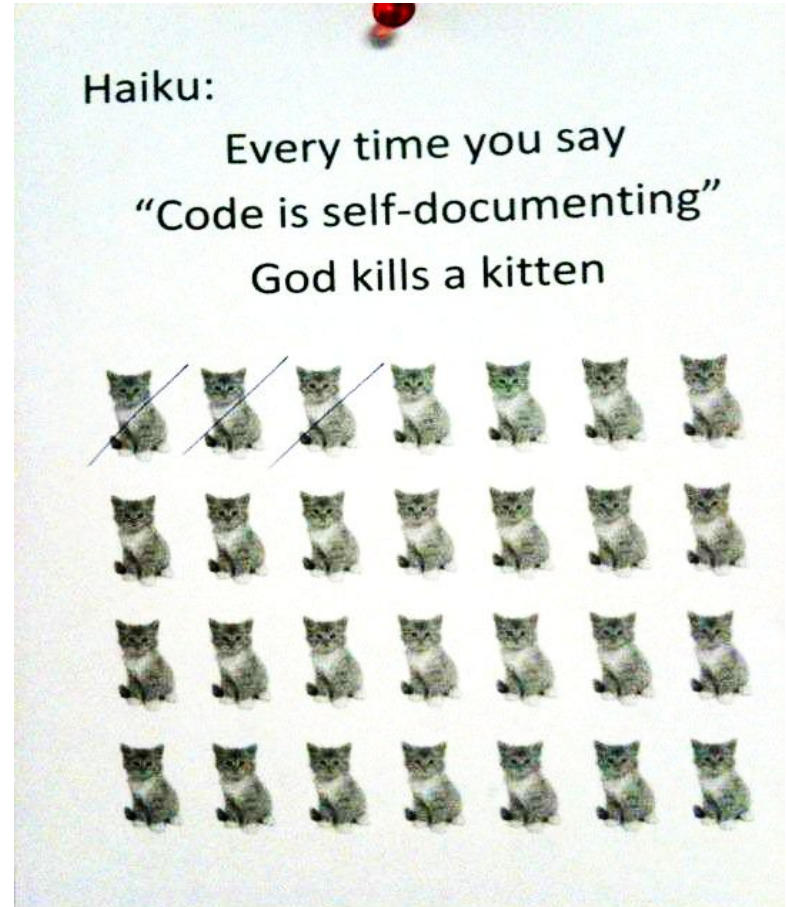
ASC
Spin Down Complete
Elapsed Time 6.015 secs
Delaying 5000 msec

Jumping to Power On Reset
```

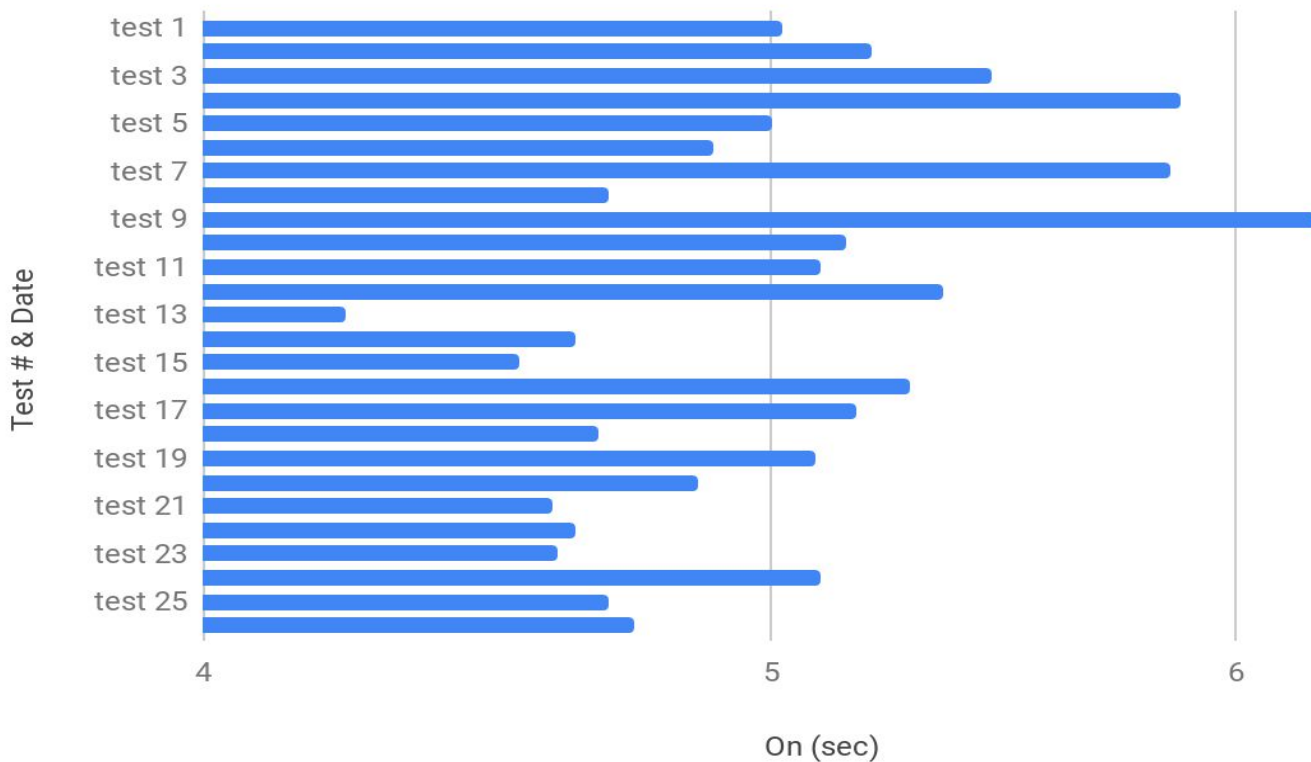
# Firmware is Weird

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++

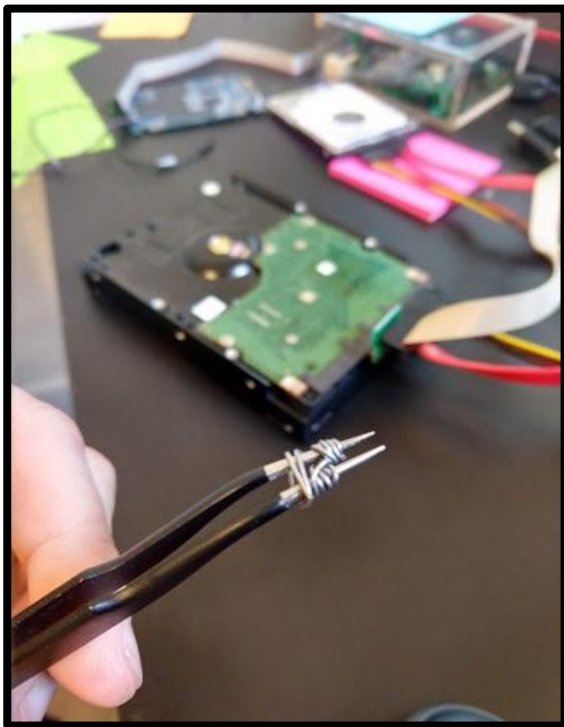
- Not all hackers are coders and not all coders are hackers
  - Exclusion of non-coders makes my hacker spirit sad
- Written to help those that don't code understand
  - Code deliberately simplistic and procedural
  - I'd like to enable everyone to learn
- Python is the lingua franca of security, C is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

# What You'll Need to DIY

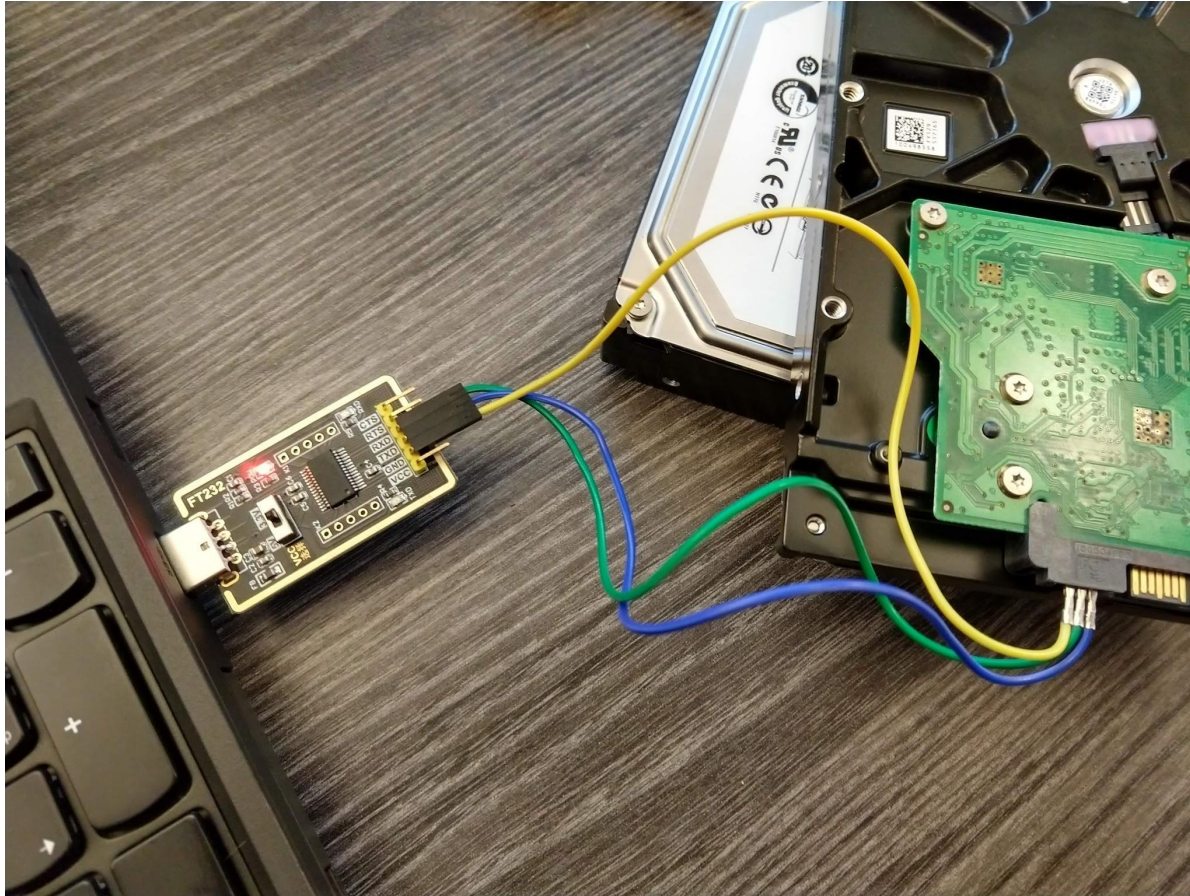
- USB to TTL Adapter with a FTDI Chip FT232RL (\$3-\$15)
- Access to the TX RX & GND pins
- Power adapter (or TTL with shared-host power)
- Code
  - <https://github.com/anaaktge/naked-trill-hdd-recovery>
  - PySerial module
- **[ENCOURAGED]** install Screen
- **[STRONGLY ENCOURAGED]**
  - Test hard drives 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

```
amn@beastie: ~  
amn@beastie: ~  
Idx LBA      PBA      LLLCHS of LBA PLPCHS of PBA SFI  Ho  
urs Msecs  Status  BBM Mask  
  
F3 T>  
ASC  
II Diag mode  
  
F3 T>  
F3 T>V4  
  
Reassigned Sectors List  
Entries: 0000, Retrieved: 0000, Alts: 0000, Removed: 0000, P  
ending: 0000, GList: 0000, RList: 0000  
  
Idx LBA      PBA      LLLCHS of LBA PLPCHS of PBA SFI  Ho  
urs Msecs  Status  BBM Mask  
  
F3 T>i4,1,22  
  
F3 T>V4  
  
Reassigned Sectors List  
Entries: 0000, Retrieved: 0000, Alts: 0000, Removed: 0000, P  
ending: 0000, GList: 0000, RList: 0000  
  
Idx LBA      PBA      LLLCHS of LBA PLPCHS of PBA SFI  Ho  
urs Msecs  Status  BBM Mask
```

```
write the V4 and read output  
results of write4  
  
num bytes returned: 0  
closing connection  
amn@beastie:~/Documents/DC_HDD_recovery_project/src$ sudo python  
clear_g-list.py /dev/ttyUSB0  
opened connection  
writing cmd: 0  
  
wrote num bytes: 3  
recv num bytes: 0  
output:  
writing cmd: V4  
  
wrote num bytes: 4  
recv num bytes: 0  
output:  
writing cmd: i4,1,22  
  
wrote num bytes: 9  
recv num bytes: 0  
output:  
writing cmd: V4  
  
wrote num bytes: 4  
recv num bytes: 0  
output:  
closing connection  
program exiting
```



# 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>