腳本小子的告白 -硬碟的秘密大公開

confessions of script kiddie - Hard Drive Secret Let Out

Who Am I?

- thx
- OSSLab 成立者
- 練過神功 所以只會硬不太會軟

我是怎樣開始踏上研究

DIY 萬歲！


SALVATIONDATA
TECHNOLOGY
www.salvationdata.com
取下音圈电机“上磁铁”
then detach the magnet in the Voice Coil Motor
0:22 / 2:50

這就是資料恢復真實成本

- 要找到一樣相容硬碟 又不保證成功率
- 碟片上有隱性刮傷
- 能Extract 的資料是否客戶要的
- 設備成本 (低塵操作環境,資料恢復設備)

簡單說 有時這跟賭博行業差不多

終極好人技已講完收工

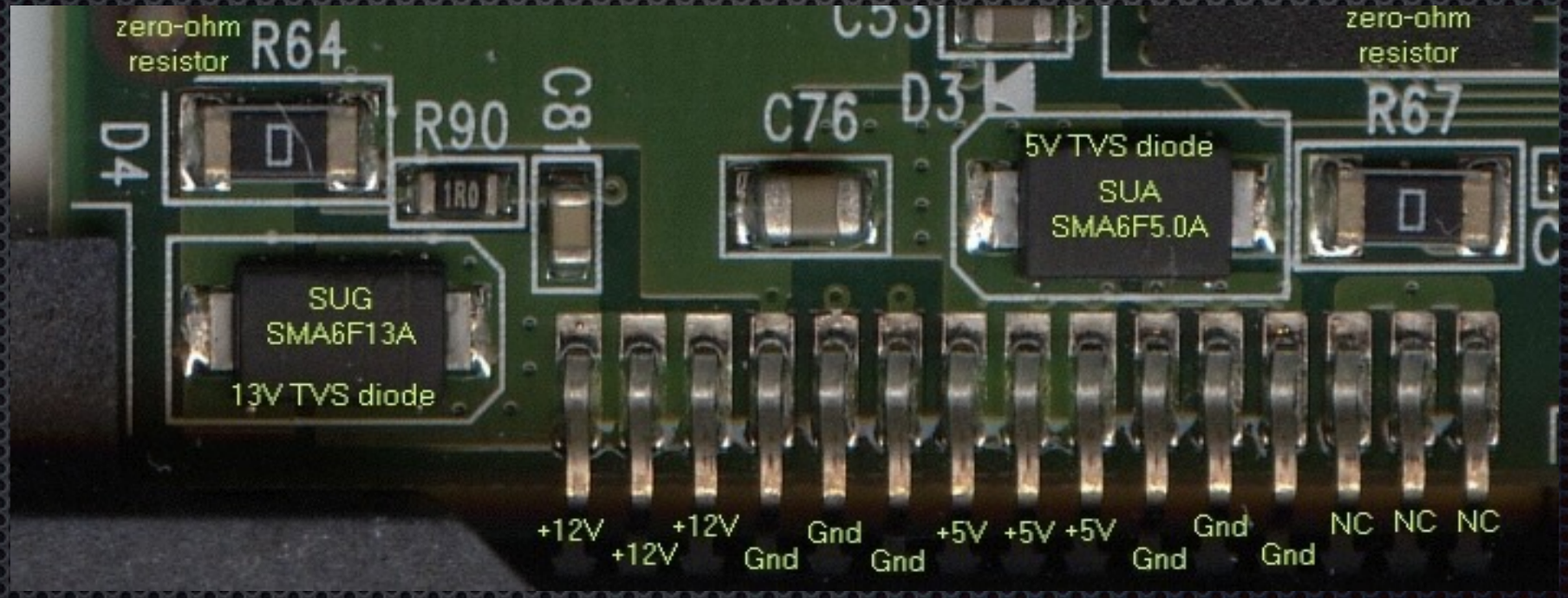
議程三分鐘 已經講完了 大家現在可散場好了 來這做行業賺錢.

向水電工學習的講師表示我當然可以超過三分鐘 這可是50分鐘議程

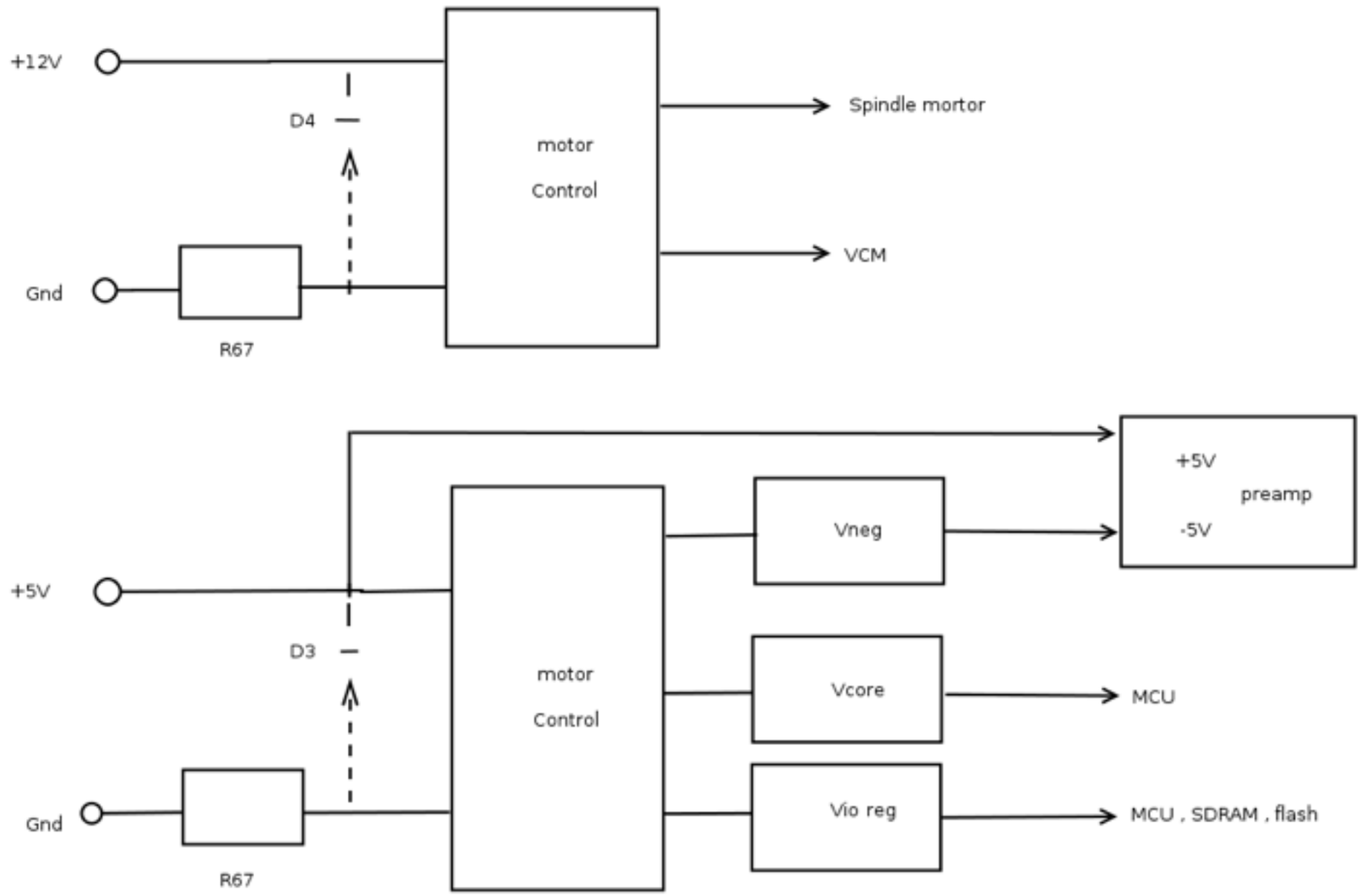
- 範例 學妹說她的硬碟IC 燒掉了
  身為一個水電工,當然隨身攜帶電表,為了學妹的資料,我掏出我的.....電表.

水電工 國中工藝課實習教學

- 拿一顆正常的硬碟 通電 ,拿出電表量就會發現 這邊要先確定GND(負極)腳位 ,再把黑針放到各接點就會發現.



分析後的硬碟電源供應圖



這樣燒掉的PCB 可修好讓它動嘛?

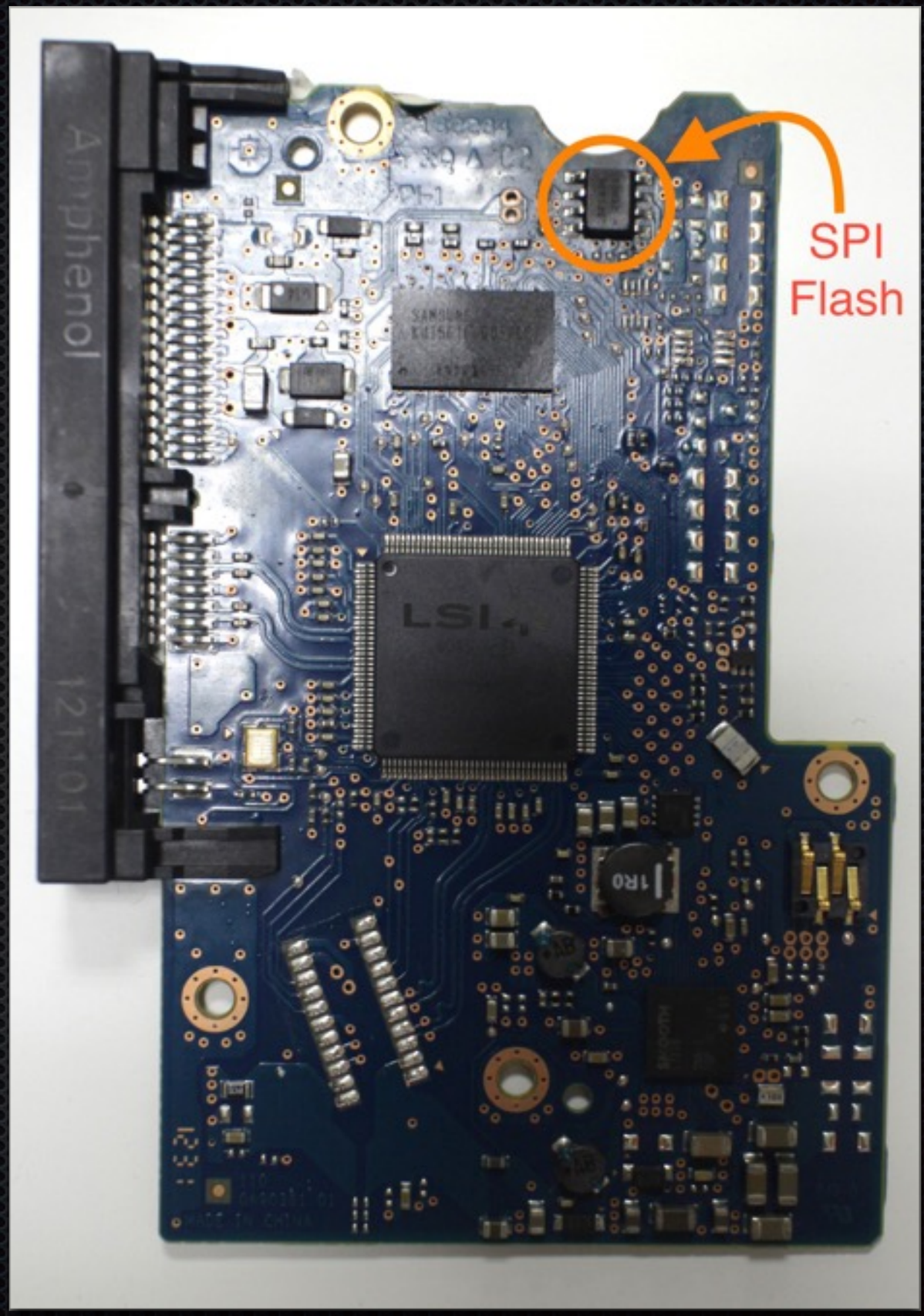
- 你看這結構, 如果5V 超壓 會怎樣?
  很有機會燒掉很多元件, 請準備砍掉重練

SPI Flash 晶片

學妹早就不在了
所以變成日立電路板
請見諒

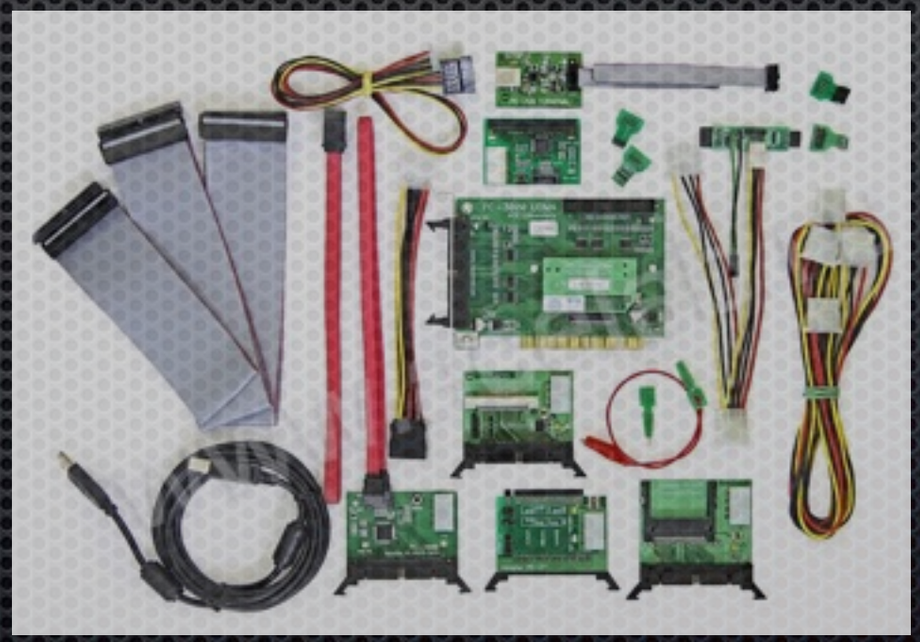
簡單說 就是壞掉那
就找那好的替換

原資料碟電路板上的
儲存性元件就要保留



我不想只做水電工可以嘛?

- 於是我買傳說中的硬碟維修設備 PC3000 http://www.acelaboratory.com/
- 這是一張很貴的PCI 卡



昂貴的資料恢復設備原理

- FPGA IC .內建ATA IP Core.並且可用於加密保護軟體不被複制
- 電源控制模塊.
- USB serial port.用於硬碟TTL終端通訊控制. 能執行工作
- 對各廠牌硬碟固件區進行讀寫操作.
- 對不良磁碟 鏡像ATA Reset, Power reset提高讀取成功率.

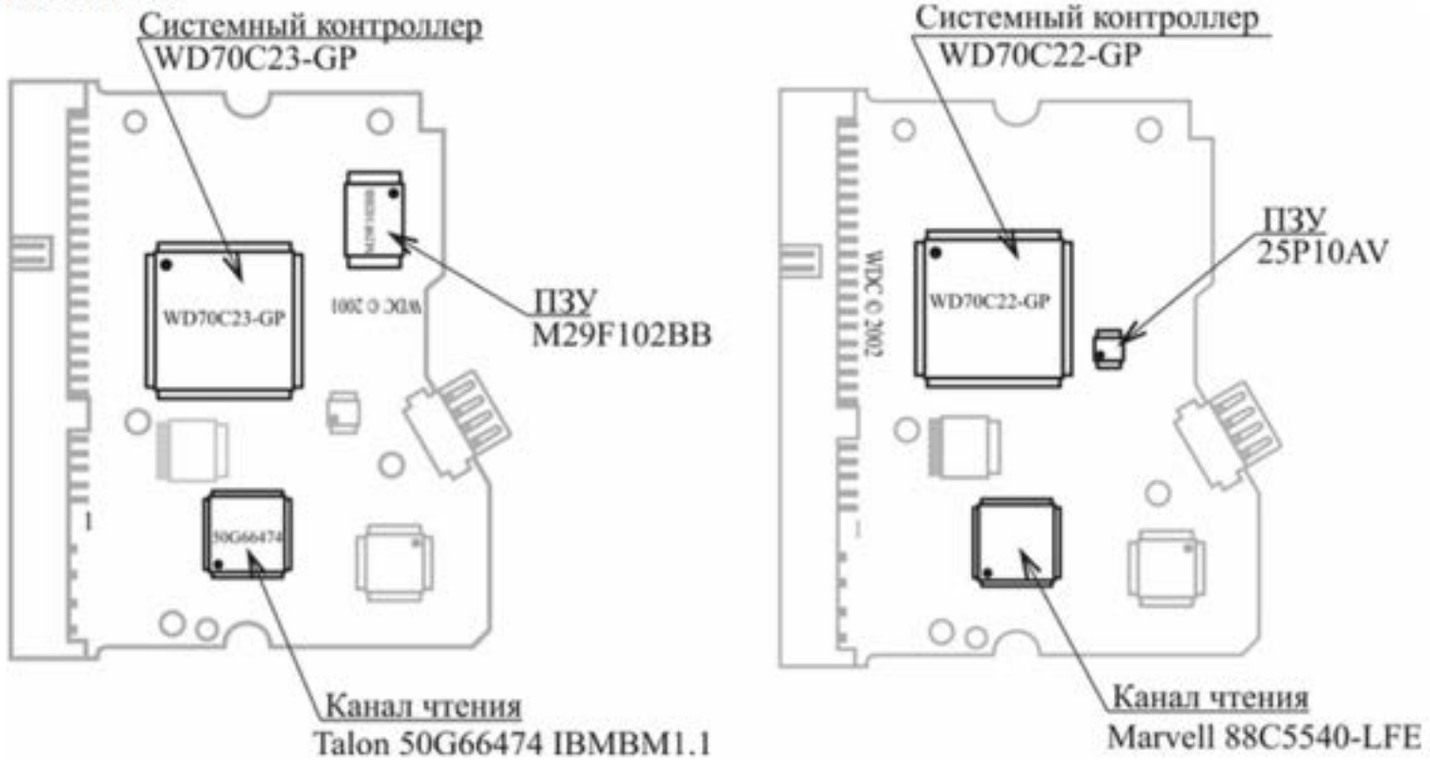
買了設備給的外星技術文件

Внимание! Тесты утилиты имеют множество настроек. Начинающим пользователям рекомендуется работать с настройками тестов по умолчанию.

4. Обзор архитектуры HDD WD.

Компания Western Digital на сегодняшний день производит две линейки накопителей, имеющих значительные различия.

Первая построена по классической архитектуре WD с использованием системного контроллера собственной разработки и берет свое начало от накопителей WD Arch-0 семейства WDC AC280 (80Мбт). Это накопители generation electronics Arch-V, Arch-VI on chip WD70Cx, имеющие максимальную емкость моделей 240 Гбт на Arch-VI:



Схемотехнический рисунок 2-х плат на WD70Cx

Вторая линейка построена на совершенно другой архитектуре с использованием системного контроллера компании Marvell 88i554x или 88i654x. Вследствие этого полностью сменились технологические команды, принцип работы со служебной зоной и технология восстановления этих накопителей. По внешнему

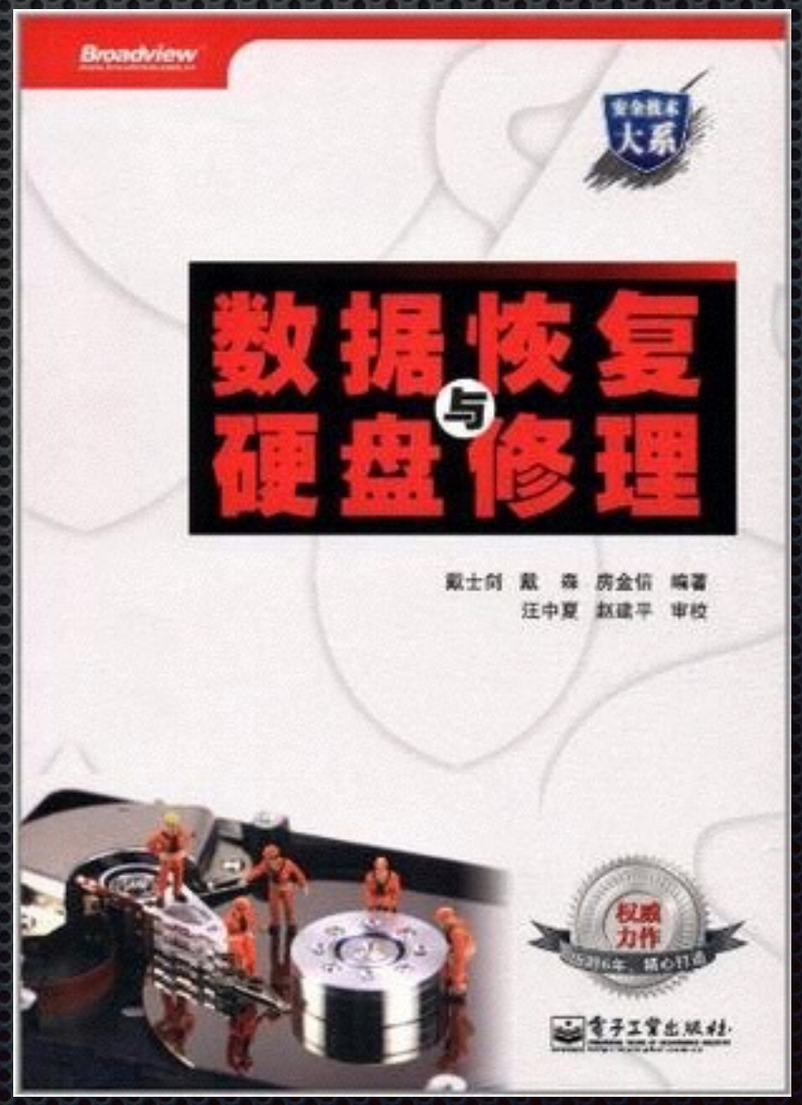
我是地球人(也沒有烏克蘭女友或老婆做我的翻譯年糕)

兔兔老婆表示震怒!!!!!!!!!!

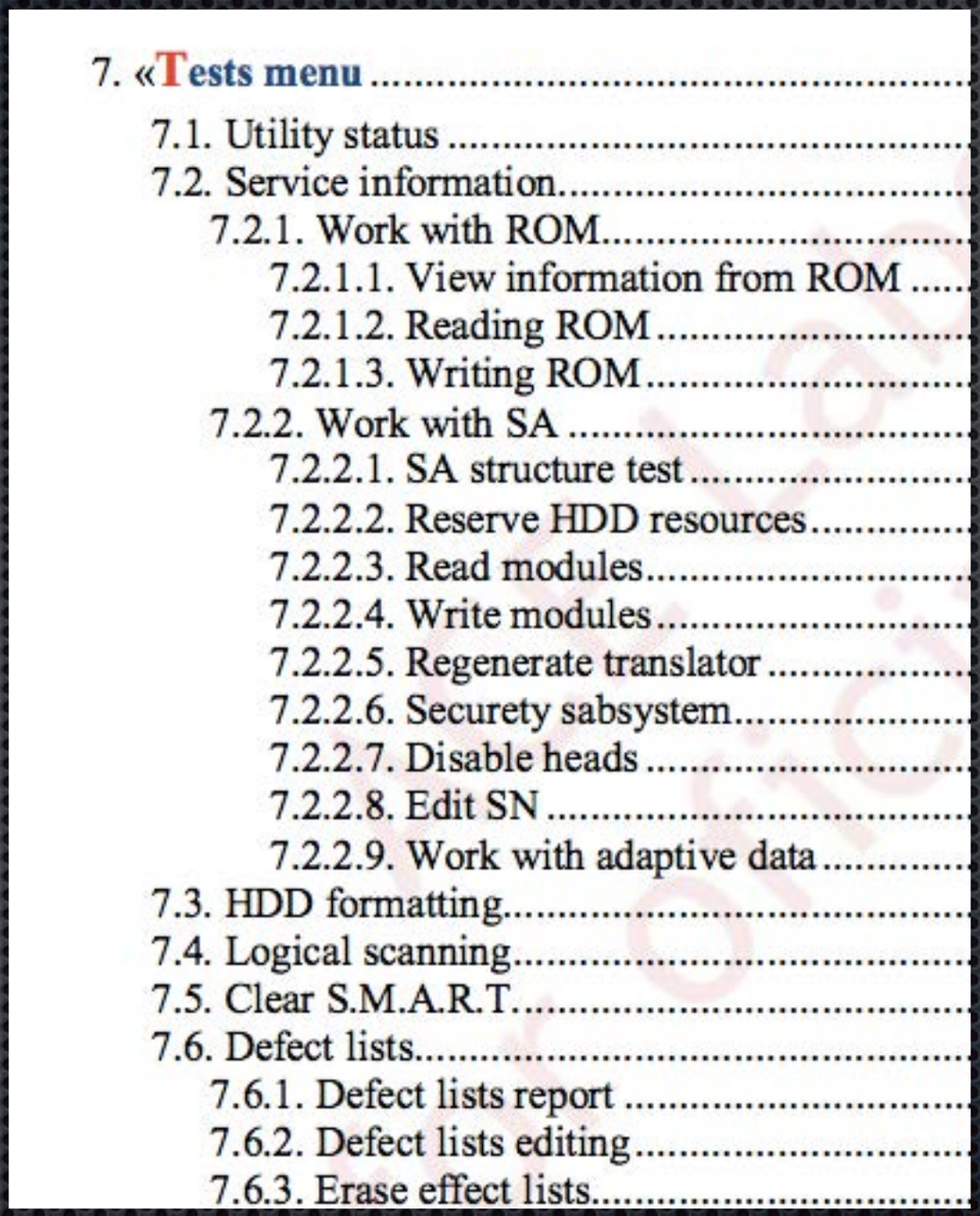
- 兔老婆說既然娶了中國老婆就要看中文的

作者有在百度百科 這本是聖經嗎?

戴士劍，2003年出版第一部數據恢復技術書，促進了數據恢復產業發展，帶動數據恢復產業
走向科學、正規、有序的發展道路



我自己弄到英文的技術手冊....



7. «Tests menu .....
  7.1. Utility status .....
  7.2. Service information.....
    7.2.1. Work with ROM.....
      7.2.1.1. View information from ROM .....
      7.2.1.2. Reading ROM .....
      7.2.1.3. Writing ROM.....
    7.2.2. Work with SA .....
      7.2.2.1. SA structure test .....
      7.2.2.2. Reserve HDD resources.....
      7.2.2.3. Read modules.....
      7.2.2.4. Write modules.....
      7.2.2.5. Regenerate translator .....
      7.2.2.6. Securety sabsystem.....
      7.2.2.7. Disable heads .....
      7.2.2.8. Edit SN .....
      7.2.2.9. Work with adaptive data .....
  7.3. HDD formatting.....
  7.4. Logical scanning.....
  7.5. Clear S.M.A.R.T.....
  7.6. Defect lists.....
    7.6.1. Defect lists report .....
    7.6.2. Defect lists editing.....
    7.6.3. Erase effect lists.....

- 對岸的國X信息中心表示,感謝台灣同胞無私的分享

司法數位鑑識人員 使用心得(一)

我們原本以為硬碟本身不需要維修，對於故障硬碟內的數據直接拷貝。硬盤出問題了要想得到裡面的data ，要先修好韌體的，才有可能進行資料拷貝，所以這方面的學習還得加強好歹我有基礎啊。看說明書，對硬盘的原理作了大堆介紹，然後對PC3000UDMA操作菜單進行了功能的說明，但隨著越來越深入的了解，而是你操作極其太復雜，簡直一不留神數據徹底變沒。

經過半月的學習，進行資料恢復過程中發現，PC3000UDMA對硬盘的多種功能處理方式都不一樣，一個功能之針對一個問題，而主要是一個功能必須結合幾個功能搭配使用，才可能有效。注意哦，是有可能有效果，那就是說也有可能無效。這不是簡單的加減法，如果關鍵地方搞錯了，你功能鍵的前後順序搞反了，那恭喜你了，你的硬盘不僅不能修復，還將徹底廢掉硬盘。而這種情況機率還相當的高，我現在也搞懂了為什麼原來拿數據出去恢復時，數據恢復公司的工程師就是不願意讓你在旁邊看，美其名曰“技術保密”，實際上是在操作失誤後方便徹底毀滅數據，讓你在其他地方都死無對證

司法數位鑑識人員 使用心得(三)

“除了複雜就是複雜”，這是我使用PC3000UDMA後的感覺。

PC3000UDMA主卡反正是我已經用了半年了，搞明白的只占三分之一，這東西除了操作復雜還需要大量的經驗，有很多說明書上說的一回事，操作起來又一回事，在我手裡光榮犧牲的硬盤不下一百塊了。但用起來還是吃力無比，這個至少搭上了我一大半的工作時間啊，有時候周末的時間都搭在上面。嚴重的投入和產出不成對比，

各位，不要以為我比你們傻，聽說公安系統的買了80套老版本的PC3000PCI的主卡回去，一年下來，只有2套還在偶爾用用，其他的直接都扔角落了，那些人不比我傻吧。

為何大家都狀況外?

- PC 3000人機介面真的很爛..
- 不夠瞭解硬碟的本質工作原理
- 硬碟有多重故障原因可能性(硬體,韌體)
- 教學人員只是個代理
- 這行不喜歡有體系的教學 想寫有體系的教學的人又沒技術..

多麼痛的領悟

- K書跟實務操作幾年 終於略懂這些技術文件在說啥

Call me Master !!!!! (快叫我大大)

對這種概念不清的又不知整個硬碟韌體架構的人.操作這些設備很容易把硬碟弄掛了..

以下部份為我本來要在企業場講的架構 現在大家聽到賺到oh !!!!

硬碟啟動流程 (以WD為範例)

- MCU ROM bootstrap
- 內部或是外在SPI ROM
- 碟片上的Module 01 Index
- 碟片上ATA 微代碼(Module 11)
- 碟片上其他完整微代碼+匹配參數

- 所以硬碟如同一個 embedd system 不同的是儲存韌體地方會二個位置ROM跟碟片

MRT应用(F) 工具(T) 窗口(W) 帮助(H)

请选择接口

ATA0 ATA1 ATA2 ATA3 IDE模式

AUTO

选择硬盘厂

常规通用功能

数据恢复功能

Western Digital

Seagate

Hitachi / IBM / HGST

Samsung

Toshiba

Fujitsu

Maxtor

专用工具模块

WDC Marvell

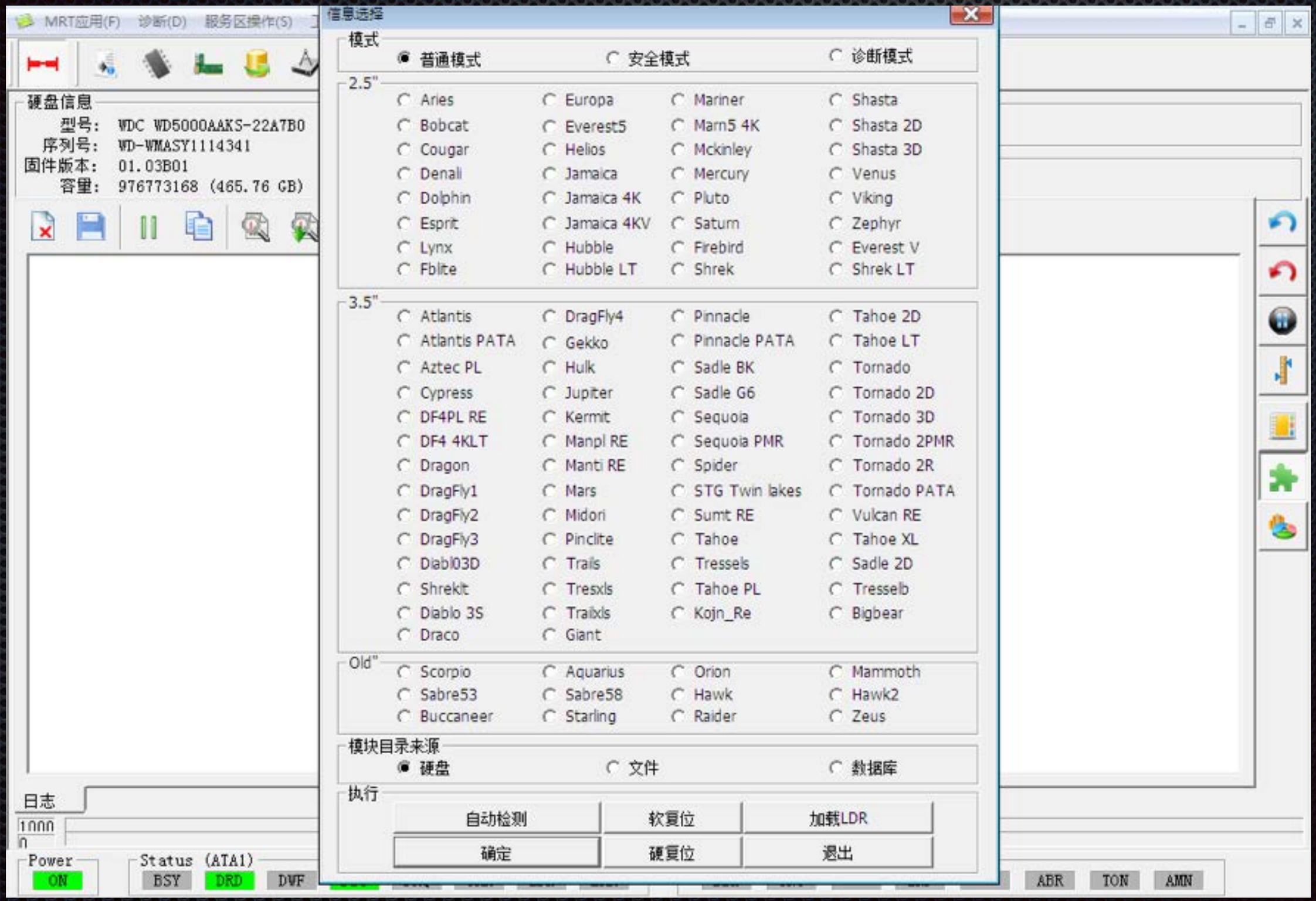
工具模块详细

支持的硬盘家族：Scorpio，Orion，Aquarius，Aries，Lynx，McKinley，Viking，Cougar，Denali，Saturn，Venus，Mercury，Shasta，Callisto，Everest，Pluto，Mariner，Dolphin，Bobcat，Jamaica，Firebird，Shasta 2D，Shasta 3D，Europa，Jamaica 4K，Marn5 4K，Zephyr，Helios，Esprit，Mammoth，Sabre53 (Sabre)，Sabre58(Unicorn)，Buccaneer，Hawk，Zeus，Raider，Starling，Hawk2，Tornado，Sequoia，Tornado PATA，Jupiter，Tornado 2D，Sequoia PMR，STG Twin lakes，Tornado 2PMR，Atlantis，Pinnacle，Hulk，Spider，Mars，Kermit，Cypress，Gekko，Atlantis PATA，Manti RE，Tahoe，Midori，Pinclite，DragFly1，DragFly2，Dragon，Manpl RE，DF4PL RE，MZTGP RE，Aztec PL，Sumt RE，Tahoe LT，Sadle BK，DF4 4KLT，Sadle G6，Draco，Sadle 2D

Power ON

Status (ATA1) BSY DRD DWF DSC DRQ CRR IDX ERR

Error BBK UNC INF ABR TON AMN


MRT应用(F)
诊断(D)
服务区操作(S)
硬盘信息
型号: WDC WD5000AAKS-22A7B0
序列号: WD-WMASY1114341
固件版本: 01.03B01
容量: 976773168 (465.76 GB)
日志
Power
ON
Status (ATA1)
BSY
DRD
DWF
ABR
TON
AMN
信息选择
模式
普通模式
安全模式
诊断模式
2.5"
Aries
Bobcat
Cougar
Denali
Dolphin
Esprit
Lynx
Fblite
Europa
Everest5
Helios
Jamaica
Jamaica 4K
Jamaica 4KV
Hubble
Hubble LT
Mariner
Marn5 4K
Mckinley
Mercury
Pluto
Saturn
Firebird
Shrek
Shasta
Shasta 2D
Shasta 3D
Venus
Viking
Zephyr
Everest V
Shrek LT
3.5"
Atlantis
Atlantis PATA
Aztec PL
Cypress
DF4PL RE
DF4 4KLT
Dragon
DragFly1
DragFly2
DragFly3
Diabl03D
Shrekit
Diablo 3S
Draco
DragFly4
Gekko
Hulk
Jupiter
Kermit
Manpl RE
Manti RE
Mars
Midori
Pinclite
Trails
Tresxls
Trailxls
Giant
Pinnacle
Pinnacle PATA
Sadle BK
Sadle G6
Sequoia
Sequoia PMR
Spider
STG Twin lakes
Sumt RE
Tahoe
Tressels
Tahoe PL
Kojn_Re
Tahoe 2D
Tahoe LT
Tornado
Tornado 2D
Tornado 3D
Tornado 2PMR
Tornado 2R
Tornado PATA
Vulcan RE
Tahoe XL
Sadle 2D
Tresselb
Bigbear
Old"
Scorpio
Sabre53
Buccaneer
Aquarius
Sabre58
Starling
Orion
Hawk
Raider
Mammoth
Hawk2
Zeus
模块目录来源
硬盘
文件
数据库
执行
自动检测
软复位
加载LDR
确定
硬复位
退出

WD 硬碟重要參數

MRT应用(F) 诊断(D) 服务区操作(S) 工具(T) 窗口(W) 帮助(H)

硬盘信息
型号: WDC WD5000AAKS-22A7B0
序列号: WD-WMASY1114341
固件版本: 01.03B01
容量: 976773168 (465.76 GB)

其它信息
家族 : Atlantis
SA Cyl : 170 Head:4 SPT:1311
ROM版本 : 02.3RC
启动模式: 普通模式

最近操作
N/A

任务信息
N/A

```
Technology mode key : .........................: OK

RAM:
Read HDD Info : ...............................: OK
Heads number : ................................: 4
Head map : ....................................: F
SA Cyl Count : ................................: 170
Serials Mark : ................................: 9D16
Control version : .............................: 45D0

Zone allocation table : .......................: OK
SA SPT : ......................................: 1311

ROM:
Read Rom Infos : ..............................: OK
ROM Data Size : ...............................: 192 Kb
ROM version : .................................: 02.3RC
ROM generation : ..............................: 02.3RC
Link table version : ..........................: 03.8H
ROM Firmware version : ........................: 0002003R

ROM Modules:
```

日志

Power ON

Status (ATA1) BSY DRD DWF DSC DRQ CRR IDX ERR

Error BBK UNC INF ABR TON AMN

ROM 微代碼版本號

MRT应用(F) 诊断(D) 服务区操作(S) 工具(T) 窗口(W) 帮助(H)

硬盘信息
型号: WDC WD5000AAKS-22A7B0
序列号: WD-WMASY1114341
固件版本: 01.03B01
容量: 976773168 (465.76 GB)

其它信息
家族 : Atlantis
SA Cyl : 170 Head:4 SPT:1311
ROM版本 : 02.3RC
启动模式: 普通模式

最近操作
诊断 -> 服务区操作 -> ROM操作 -> ROM列表

任务信息
N/A

ROM列表 4F.bin

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	52	4F	59	4C	04	00	1F	00	4F	00	01	00	F1	5F	43	11	ROYL....O...._C.
00000010	30	30	30	32	30	30	33	52	00	00	00	00	00	00	00	00	0002003R........
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000050	55	AA	04	00	E1	46	FC	46	29	47	04	47	00	00	00	00	U....F.F)G.G....
00000060	00	00	00	00	55	AA	04	00	1F	FC	6D	E9	DB	FF	18	FB	....U.....m.....
00000070	EC	FF	24	00	2D	00	F7	FF	C3	FF	FD	FF	45	06	51	EA	..$.-.......E.Q.
00000080	FA	FF	28	FB	F7	FF	D2	FF	EA	FF	C9	FF	09	00	F3	FF	..(.............
00000090	E3	02	9C	EA	09	00	92	FB	0B	00	61	00	16	00	46	00	..........a...F.
000000A0	05	00	18	00	92	08	C0	E3	75	FF	91	FB	18	00	0C	00	........u.......
000000B0	34	00	C5	FF	F2	FF	1B	00	00	00	00	00	00	00	00	00	4...............
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

B:50 W:12338 DW:858796082 | Pos:13 (19) | 19 - 23 (5) | ID:4F Size:1

日志 ROM对象

Power: ON

Status (ATA1): BSY DRD DWF DSC DRQ CRR IDX ERR

Error: BBK UNC INF ABR TON AMN

啥是模塊..(module)

- 模塊是硬碟碟片上韌體跟匹配參數分類
- 比如說 序號,型號 ,ATA 密碼是存在專門模塊.而不是在 PCB .
- 有分重要級數 重要模塊一丟私 資料一去不復反

MRT应用(F) 诊断(D) 服务区操作(S) 工具(T) 窗口(W) 帮助(H)

硬盘信息
型号: WDC WD5000AAKS-22A7B0
序列号: WD-WMASY1114341
固件版本: 01.03B01
容量: 976773168 (465.76 GB)

其它信息
家族 : Atlantis
SA Cyl : 170 Head:4 SPT:1311
ROM版本 : 02.3RC
启动模式: 普通模式

最近操作
工具 -> 固件区对象查看 -> 模块列表

任务信息
N/A

模块列表

以ID方式操作模块时，将按ID号自动对Copy0，Copy1分别进行操作

模块ID	重要级别	长度(扇区)	说明	读	头部	校验
0001	B	0018	Modules directory			
0035	Dd	000A	SA Defects			
00C1	Dr	0001	Calibrations module			
0033	Dd	039E	P-List (Primary defec...			
0031	Ad	0255	Translator			
000C	B	0005	Models table			
0034	C	0017	G-List (Grown defect ...			
0032	Ad	0020	Relo Bad Block Module			
0036	Ad	0009	T-List Module			
0029	B	0006	microprogram code			
0040	As	007D	Adaptive data			
0041	As	007D	Adaptive data			
0042	As	007D	Adaptive data			
0043	As	007D	Adaptive data			
004E	B	004C	microprogram code			
0049	As	0003	Adaptive data			
004A	As	001A	Adaptive data			
004D	As	0001	Adaptive data			
0003	As	001C	Format Select Data Mo...			
0004		0311	Family models configu...			
0025		0101				

日志 ROM对象 模块对象

Power ON

Status (ATA1) BSY DRD DWF DSC DRQ CRR IDX ERR

Error BBK UNC INF ABR TON AMN

有必要的中斷

- 剛剛已經講完硬碟boot 流程,任何一塊錯了 就有機會造成硬碟”當機”
- 所以說打斷 不正確的開機Boot步奏是很重要的
- ROM 有碟片韌體區缺陷位置 修改他 可以造成流成上的中斷
- 打斷後 基本狀況下 可以讀寫韌體區.可嘗試修理韌體或是將重要模塊備出.以其他硬碟啟動載入重要模塊.再做熱交換

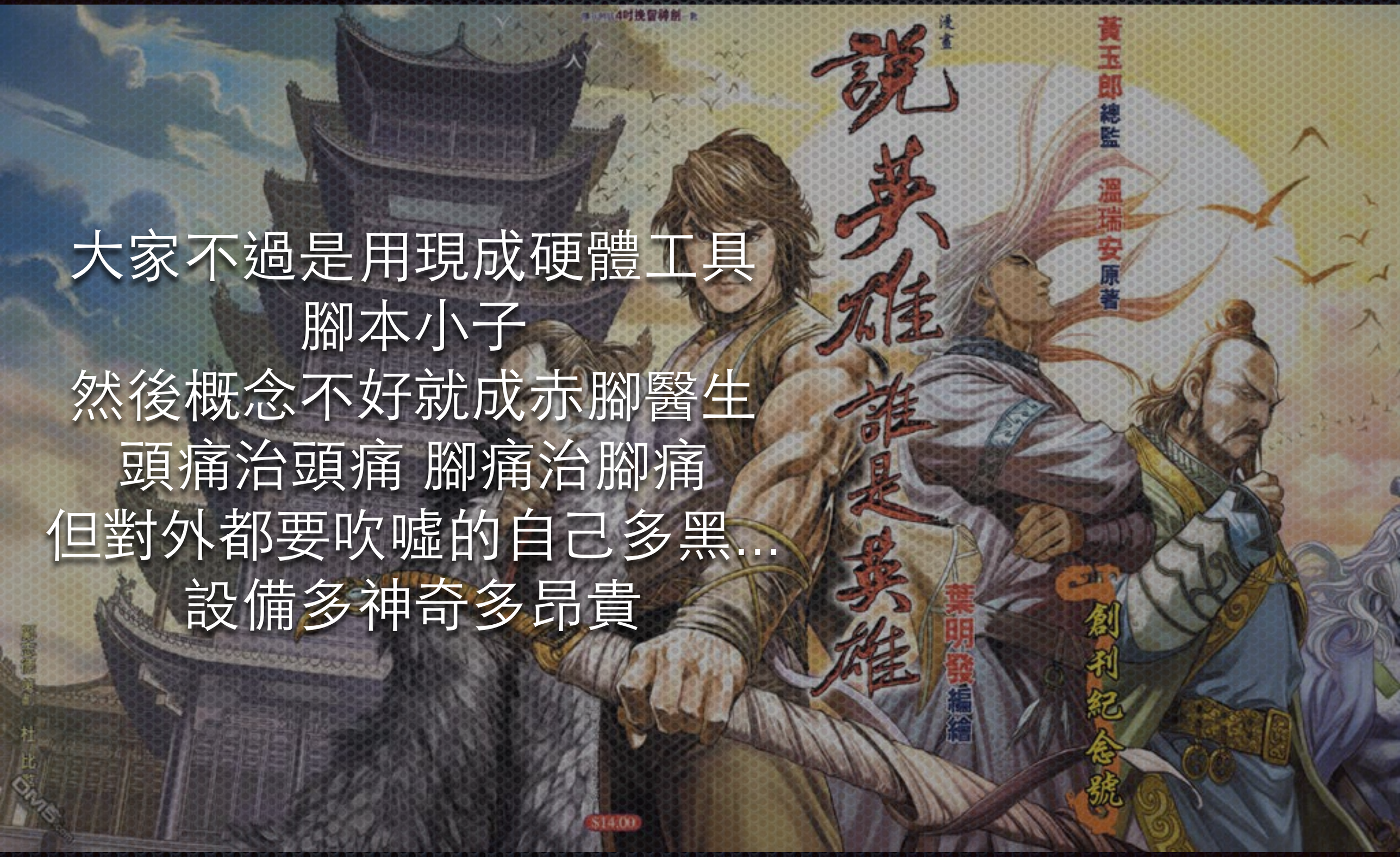
韌體跟資料恢復的關系

- 硬碟容易硬體與韌體一起故障
- 增加Dinor材料硬碟相容性
- 讓硬碟在極限狀態讀取資料

這樣算真硬體 Hacker嗎?

真相是 我只是比較”熟練”的 Program Kiddle

說黑黑 誰是真黑黑?



大家不過是用現成硬體工具
腳本小子
然後概念不好就成赤腳醫生
頭痛治頭痛 腳痛治腳痛
但對外都要吹噓的自己多黑...
設備多神奇多昂貴

ATA Vendor-specific command

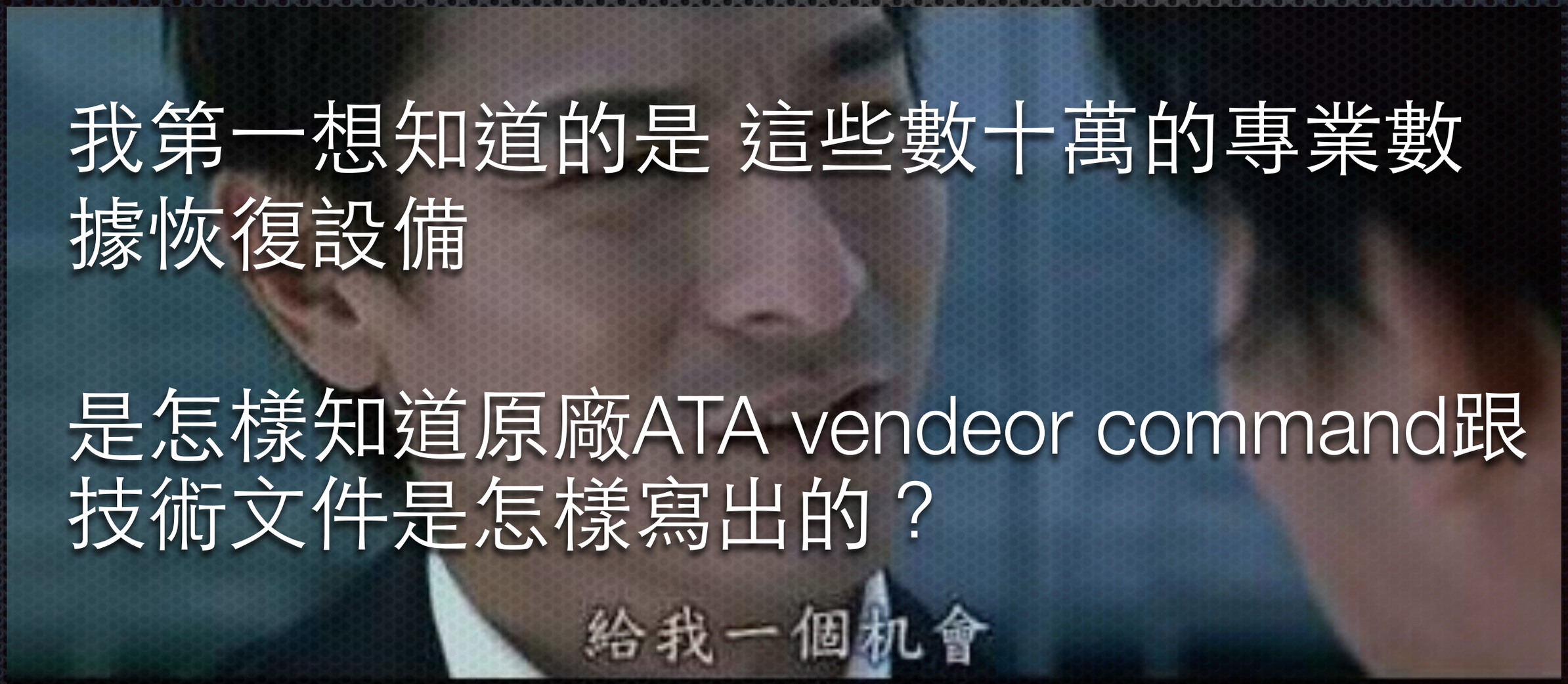
- 公開的T10 文件就有寫了
  Something (e.g., a bit, field, or code value) that is not defined by the standard and may be used differentlyn various implementations.
- This proposal defines a SCSI 16 byte CDB for issuing an ATA command, and sense information to report completion status. This mechanism allows.

CDB (Command Descriptor Block)

16-byte CDB:

bit→ ↓byte	7	6	5	4	3	2	1	0
0	Operation code = 03h							
1	LUN			Service Action				
2	Logical Block (MSB)							
3								
4								
5	Logical Block (LSB)							
6	Addition CBP information							
7	Addition CBP information							
8	Addition CBP information							
9	Addition CBP information							
10	Allocation length (MSB)							
11								
12								
13	Allocation length (LSB)							
14	Misc. CDB data							
15	Control							

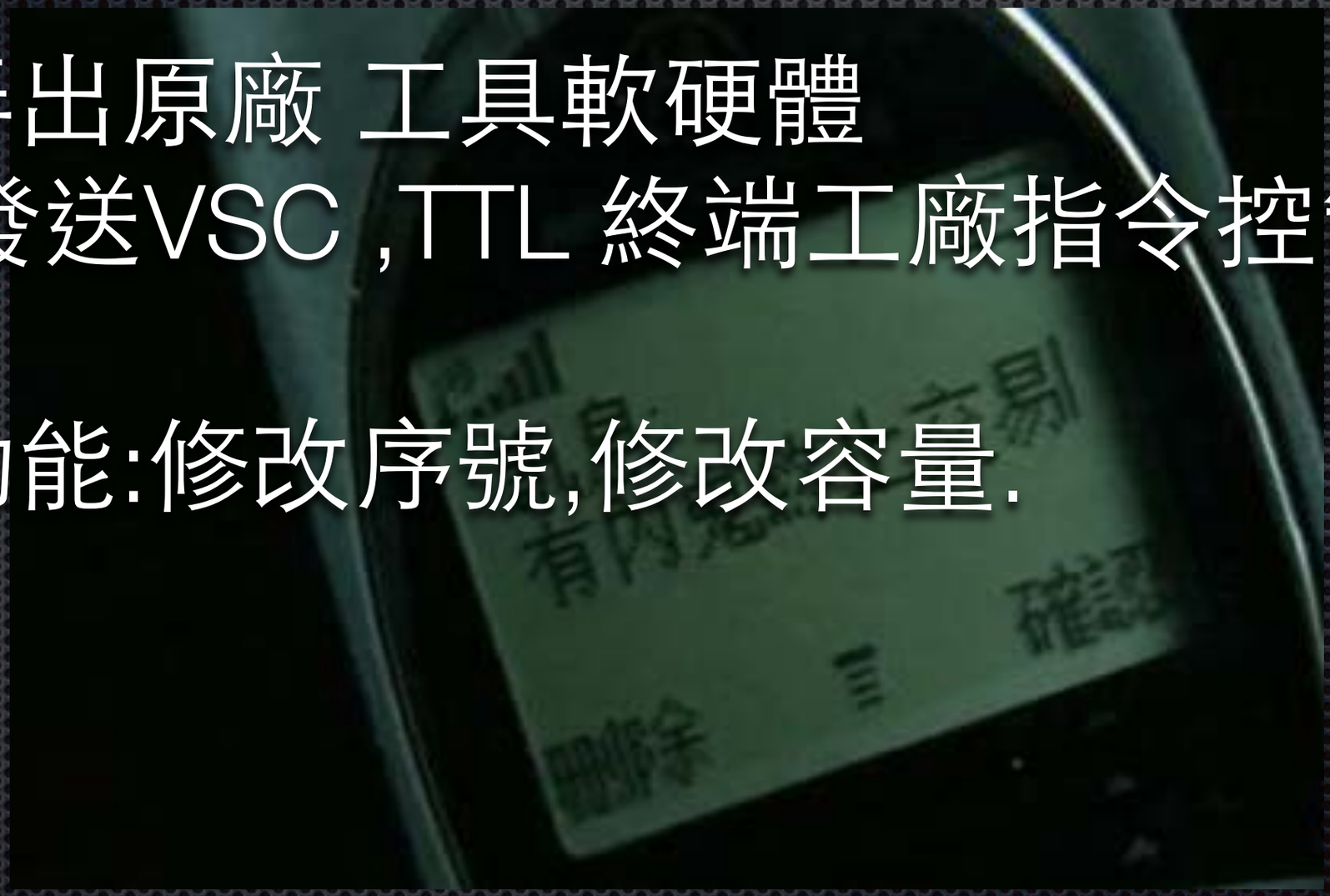
給我一個機會 我想做黑黑(好人)



我第一想知道的是 這些數十萬的專業數據恢復設備

是怎樣知道原廠ATA vendeor command跟技術文件是怎樣寫出的？

結果是這樣的:黑黑(好人)後面都有內鬼



弄出原廠 工具軟硬體
(發送VSC ,TTL 終端工廠指令控制硬碟)

功能:修改序號,修改容量.

沒內鬼 我獨立研究 可嗎?吾道不孤 (有Google)

- 嗯 我想找 WD ATA Vender Command 相關資訊

從世上最大的黑硬體市場“游戲機”說起

- 遊戲機是這世上被硬體hacking比例最高的硬體....
  在亞洲市場被黑過的比沒黑過的還多!!!!

市場大 ,因此有人做了一些研究 :
Xbox 360 專用WD 硬碟 有特制韌體,你不能隨便拿顆更大容量WD 硬碟插上去.

民之所慾 黑之所向

http://www.users.on.net/~fzabkar/HDD/HddHackr_how_it_works.txt

HddHackr reads the HDD firmware version, serial number, model number, and capacity in LBAs from sector 16 of the original Xbox HDD, and then writes this information to a supported WD drive of equal or larger capacity. It does this by using WD's vendor specific commands (VSC) to modify the HDD's firmware. AIUI, in the case of a ROYL drive, the relevant firmware modules are 0D and 02. The result of this hack is that the WD drive then identifies itself in the same way as the original drive

WD 模塊結構分析

```
MOD 0D --- contains firmware version
=================================================================
0000  52 4F 59 4C 04 00 1E 00-0D 00 01 00 1F FF 0C 3F   ROYL...........?
0010  30 30 30 31 30 30 30 30-00 00 00 00 00 00 00 01   00010000........
0020  31 31 2E 30 31 41 31 31-00 01 03 01 00 00 50 01   11.01A11......P.
0030  4E E2 01 AD 6F FB 00 01-FE FF 00 00 00 00 00 00   N...o...........
0040  01 00 00 00 00 00 00 00-00 00 64 00 00 00 00 00   ..........d.....
=================================================================


MOD 02 --- contains serial number, model number, capacity in LBAs (and passwords?)
=================================================================
0000  52 4F 59 4C 01 00 30 00-02 00 03 00 30 75 7B EC   ROYL..0.....0u{.
0010  30 30 30 38 30 30 30 30-09 1D 09 00 00 00 00 00   00080000........
...
02A0  33 00 4E 04 02 00 00 01-57 44 2D 57 58 45 36 30   3.N.....WD-WXE60
02B0  38 50 4C 37 31 30 39 00-00 00 00 00 00 01 10 3F   8PL7109........?
02C0  00 00 00 00 6F 59 1C 1D-6F 59 1C 1D 6F 59 1C 1D   ....oY..oY..oY..
02D0  6F 59 1C 1D 00 01 A4 03-00 00 00 00 07 7F 00 00   oY..............
...
04D0  00 00 00 00 01 57 44 43-20 57 44 32 35 30 30 42   .....WDC WD2500B
04E0  45 4B 54 2D 30 30 46 33-54 30 20 20 20 20 20 20   EKT-00F3T0
=================================================================
```

現在你可以自由更換更大容量硬碟了

OSSLab Easy SA Tool （硬碟韌體讀寫工具）

- 只能走主機板上SATA port.USB to SATA 穿透還在處理
- 只支持舊款WD 硬碟
- Linux 下 要先知道 ACHI port (先下lsipci)
- 只是好玩 ...(我怕有人拿來放了啥糟糕物 別害我)

Service area 實驗驗證

- Sectors Per Track (韌體區）
  磁道扇區數韌體區的每一磁道的扇區數量

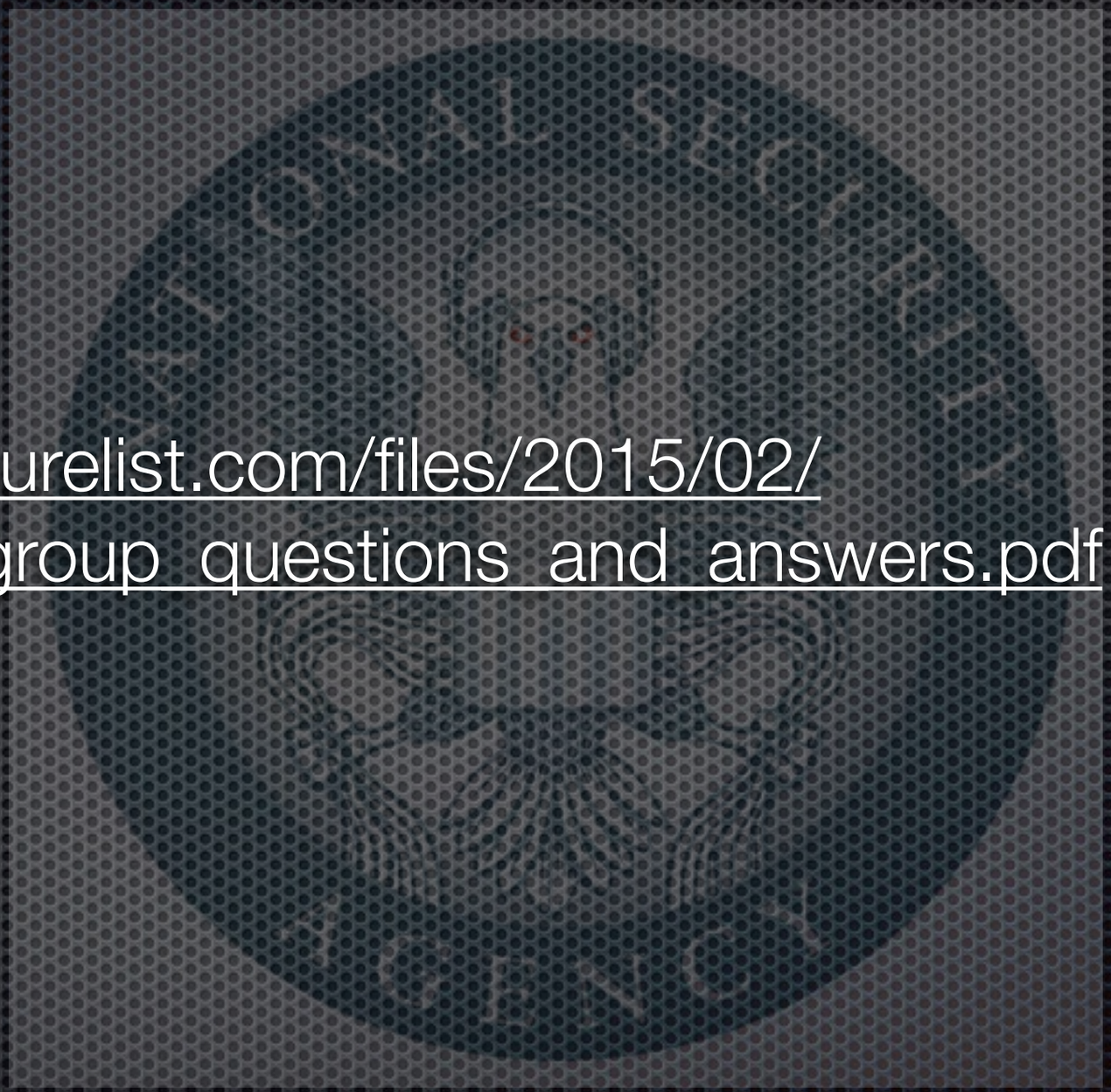
- WD2500KS-00MJB0 SPT :720　Head:6　Tracks (SA CYL): 64
  空閒韌體區總共大小 4x 64 x 720 x 512b byte=96MB
  大小　（0,1 主頭軔體區用於存放硬碟微代碼跟匹配參數)

- 做完低階格式化. 這區的資料還在嗎?

Easysa 操作方法

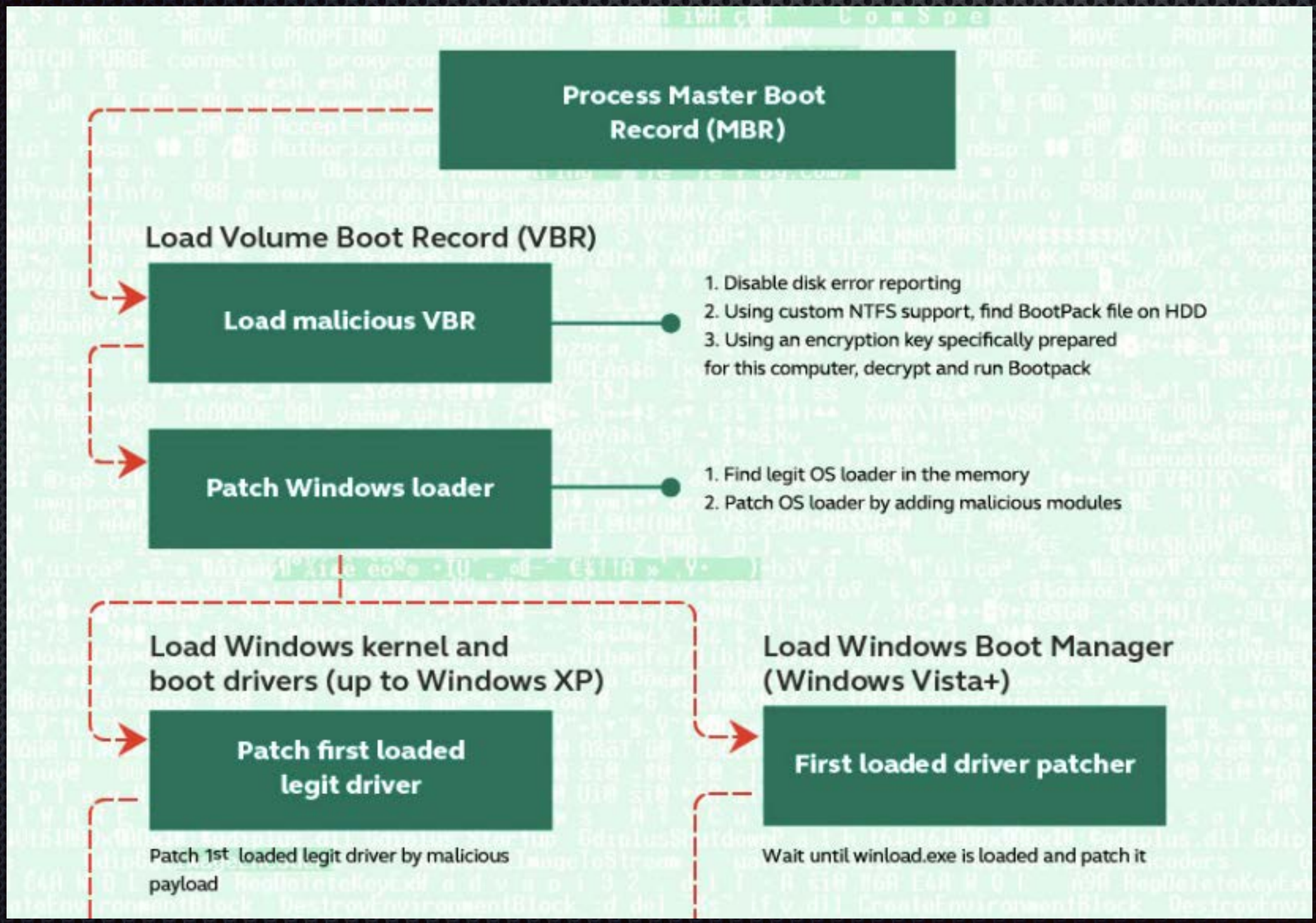
- dd if=/dev/urandom count=184320 > random-file ; md5sum random-file
- ./easysa -p 0x0170 -w ./random-file
- dd if=/dev/zero of=/dev/sdb bs=1M
- ./easysa -p 0x0170 -r after-dding-dev-zero
- md5sum after-dding-dev-zero

老大哥就是這樣看著你



- https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

史上最先進病毒


Process Master Boot Record (MBR)
Load Volume Boot Record (VBR)
Load malicious VBR
1. Disable disk error reporting
2. Using custom NTFS support, find BootPack file on HDD
3. Using an encryption key specifically prepared for this computer, decrypt and run Bootpack
Patch Windows loader
1. Find legit OS loader in the memory
2. Patch OS loader by adding malicious modules
Load Windows kernel and boot drivers (up to Windows XP)
Patch first loaded legit driver
Patch 1st loaded legit driver by malicious payload
Load Windows Boot Manager (Windows Vista+)
First loaded driver patcher
Wait until winload.exe is loaded and patch it

韌體防火牆 Firmwall

- https://www.os3.nl/_media/2013-2014/courses/ot/jan_niels.pdf

- 軟體有防火牆,韌體也有防火牆
  預防有軟體有開啟VSC

Service Area 其他應用

- NSA 可以用 你為何不能用? 當被抄水表時,把所有主頭 (0,1頭) Service area 填0....

- 結果你知的....

Serial TTL (UART)通訊應用

- Serial UART 應用：
  - Linux 終端操作
  - 路由器或者 ADSL 韌體升級。
  - 硬碟低階操作維修。
  - 單晶片（MCU）程式下載，如STC 51單晶片。
- 需要的線材與工具
  - 杜邦接頭(母)， 1P 的三根
  - 莫士端子(母) 2.0mm，4P 排座
  - USB to TTL 板 (拿Arduino 也可替代)

Serial UART 接線對應方式

Embedded	USB to TTL版
莫式端子4P排座	杜邦接頭1Px3
GND	GND
Rx	Tx
Tx	Rx

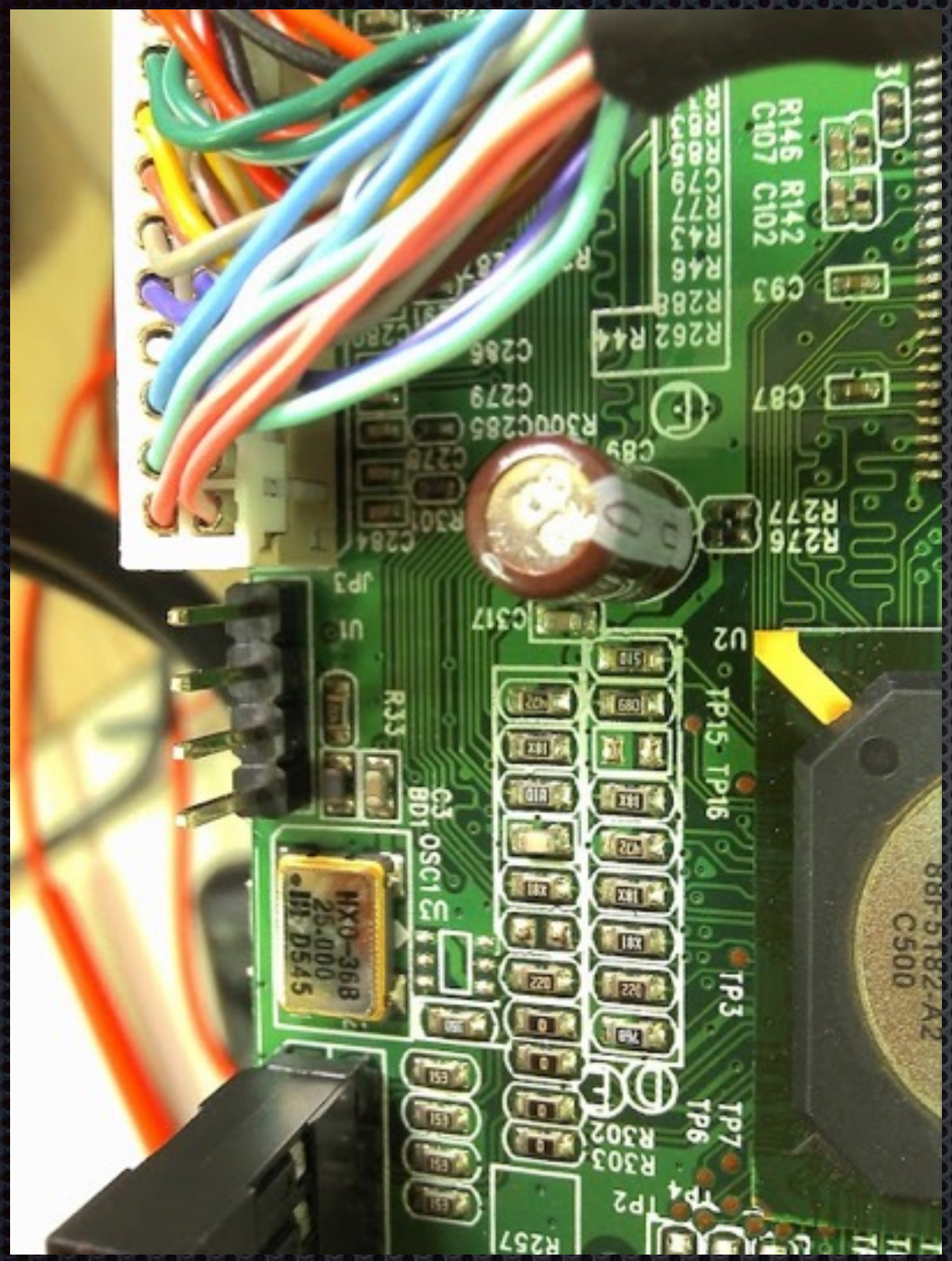
USB to UART 驅動與終端

- 驅動程式
  - Windows
  - Prolific PL2302, WinXP Driver
  - Linux
  - 已內建於 Linux kernel。
- 連線軟體
  - Windows
    - Putty
  - Linux
    - minicom on Ubuntu 12.04)

```
sudo apt-get install minicom
sudo chmod 0777 /dev/ttyUSB0
sudo minicom -s
```

TIPs:
設定 minicom:
- 序列埠設定 >
A 序列設備：/dev/ttyUSB0
E Bps/Par/Bits：115200 8N1
F 硬體Flow控制：否
G 軟體Flow控制：否

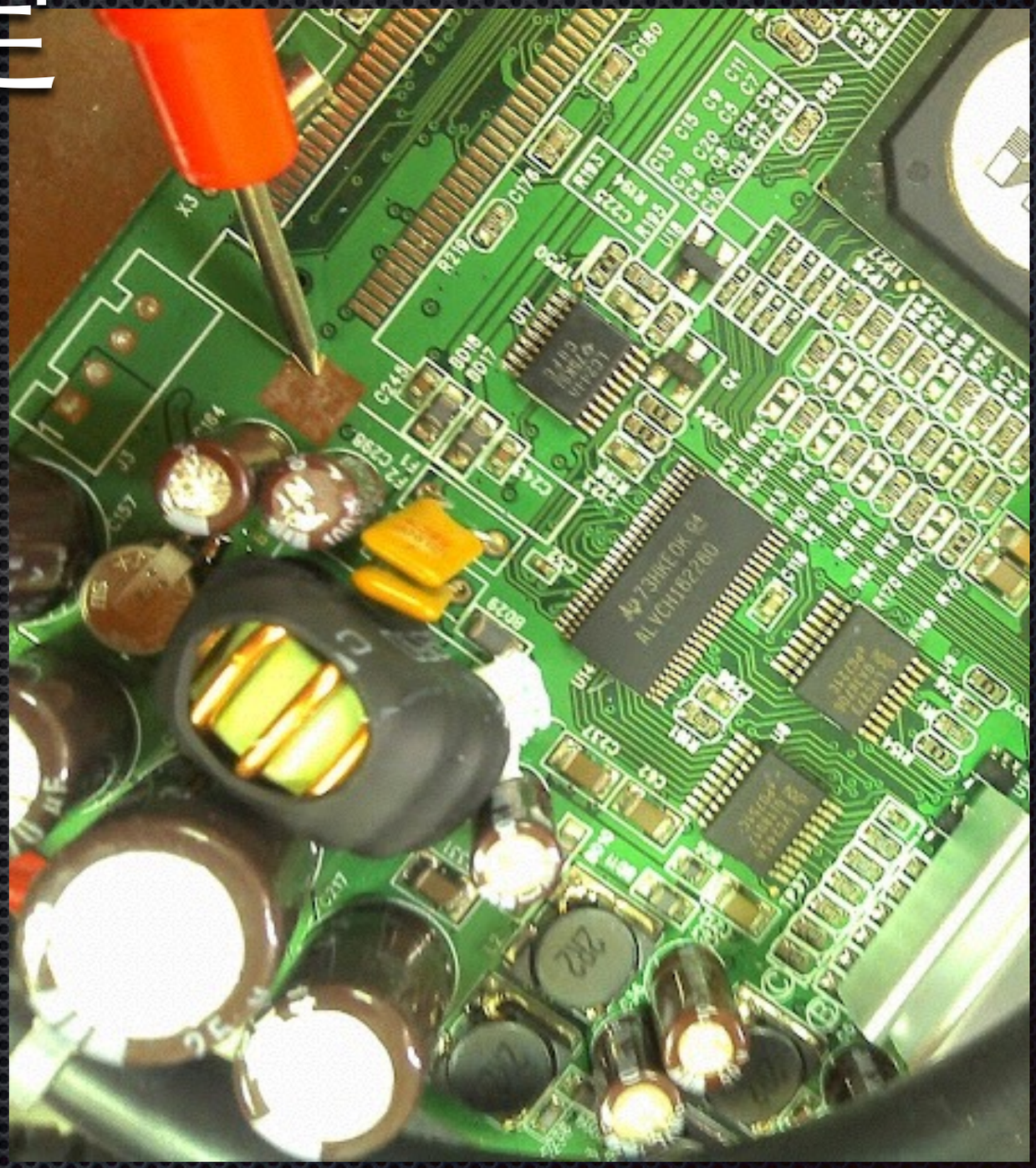
逆向 Serial UART 腳位



- 這是一台ARM NAS .

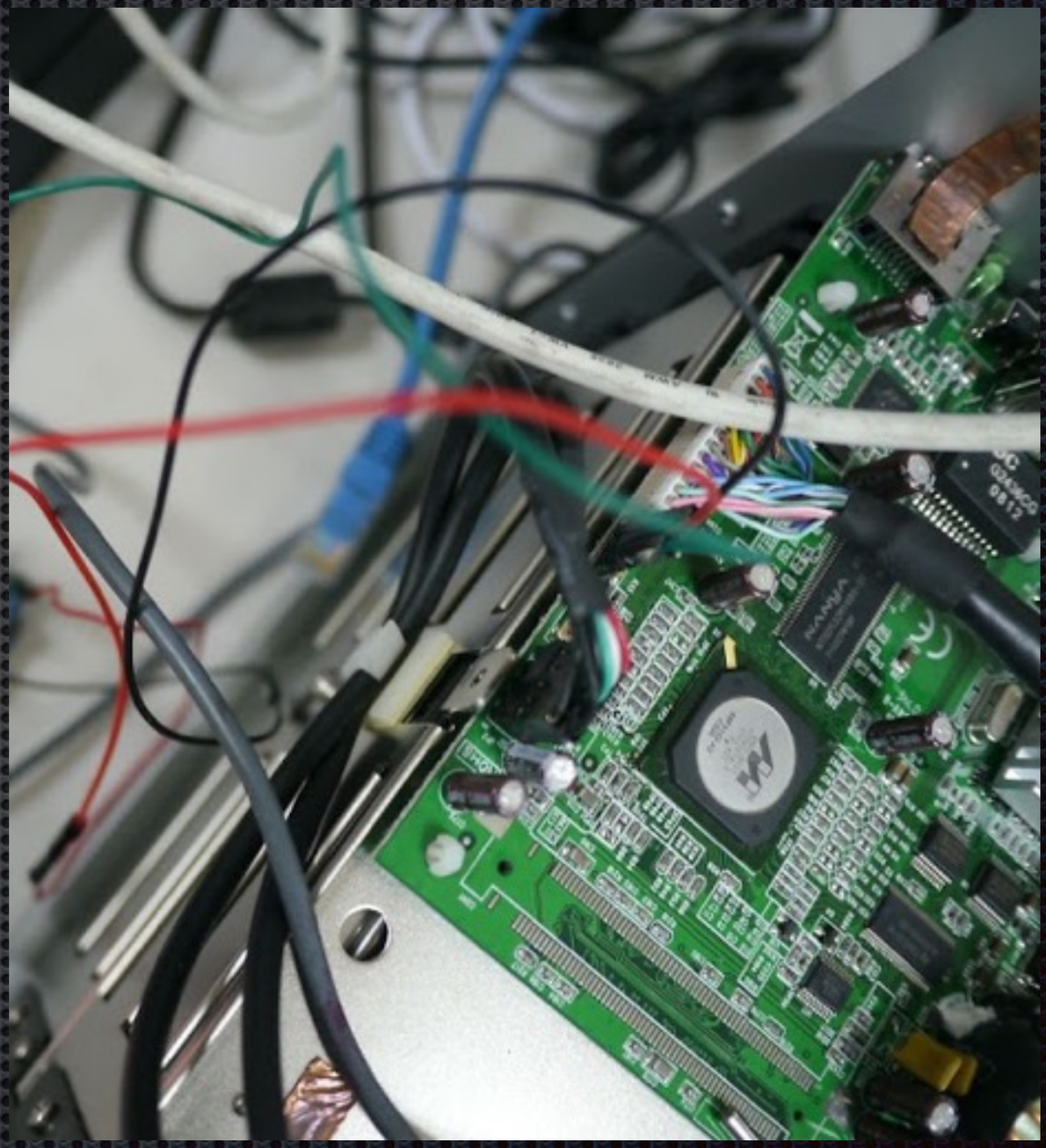
GND 腳位判定

- 最好抓的是GND
- 先將 embedded system 斷電 GND 一是大塊金屬點 或是電源座負極.會導通 數位型三用電表轉到 二極體測試檔位 (可做導通測試 有通會發聲)
- 另外一邊探針 則每個pin都試 發現第一根有跟接地點導通, 會翁鳴 。
  因此第一根為**GND**

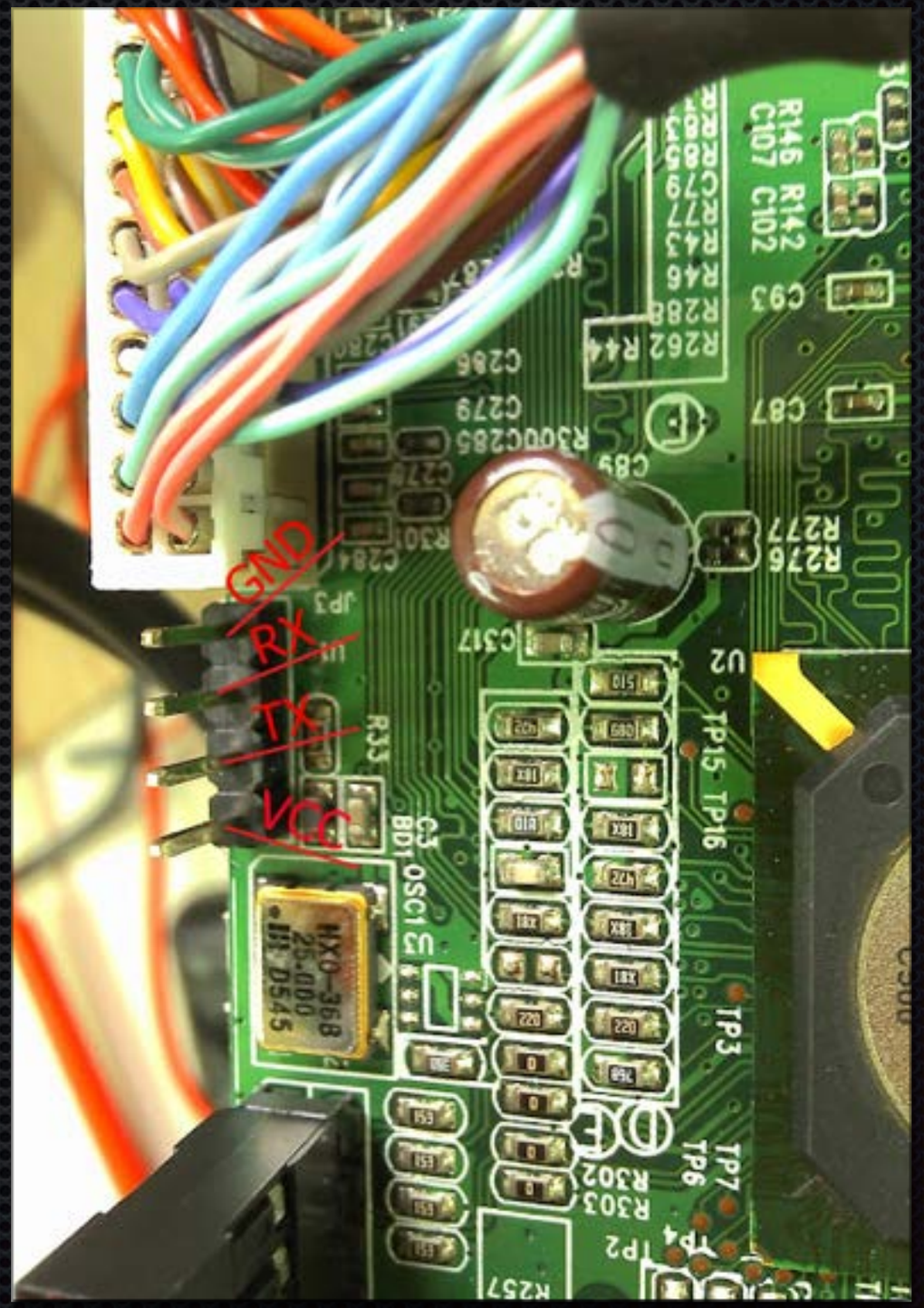


- 這時embedded system 再通電
  把探針一根固定放 GND 測試每根與第一根已知 (GND)
  相通電呀 發現當 1,4 腳位通電時 3.3V 或5V

- 表示第四根為 VCC
  RX TX , 就為中間二根。
  先顯示有字串再調速度
  用2400 ~ 115200 慢慢
  試



分析出腳位


GND
RX
TX
VCC
R146
C107
R142
C102
C93
C87
R276
R277
C317
U2
TP15
TP16
TP3
TP7
TP6
R303
R302
JP2
R257
C3
BD1
OSC1
HX0-368
25.000
JH D545

Arduino 做起黑黑應用比電子花車藝術實在多了

紅外線訊號抓取模擬發射

Apple Magicsafe 協議分析

Apple Battery Firmware Hack

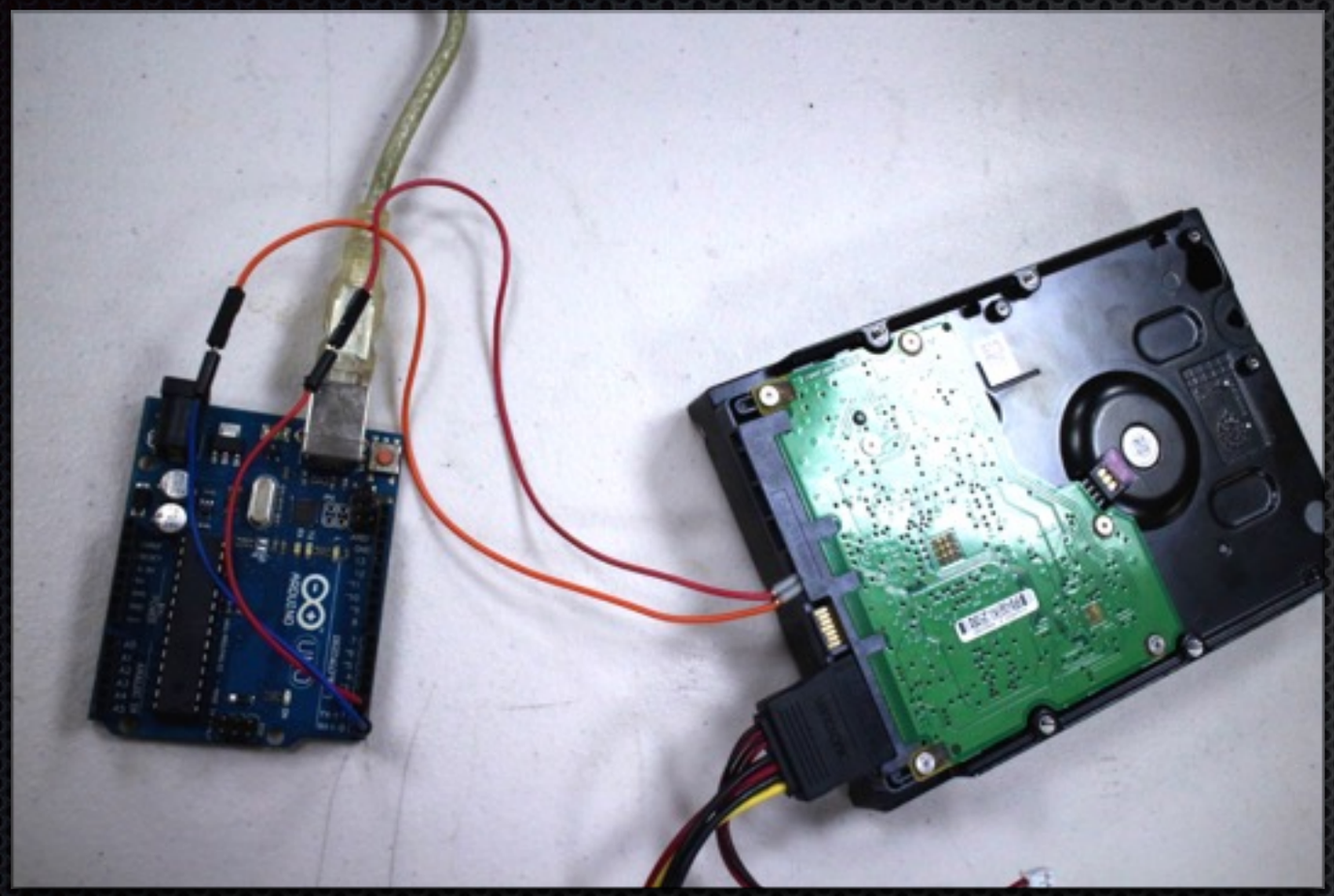
Bios 密碼破解

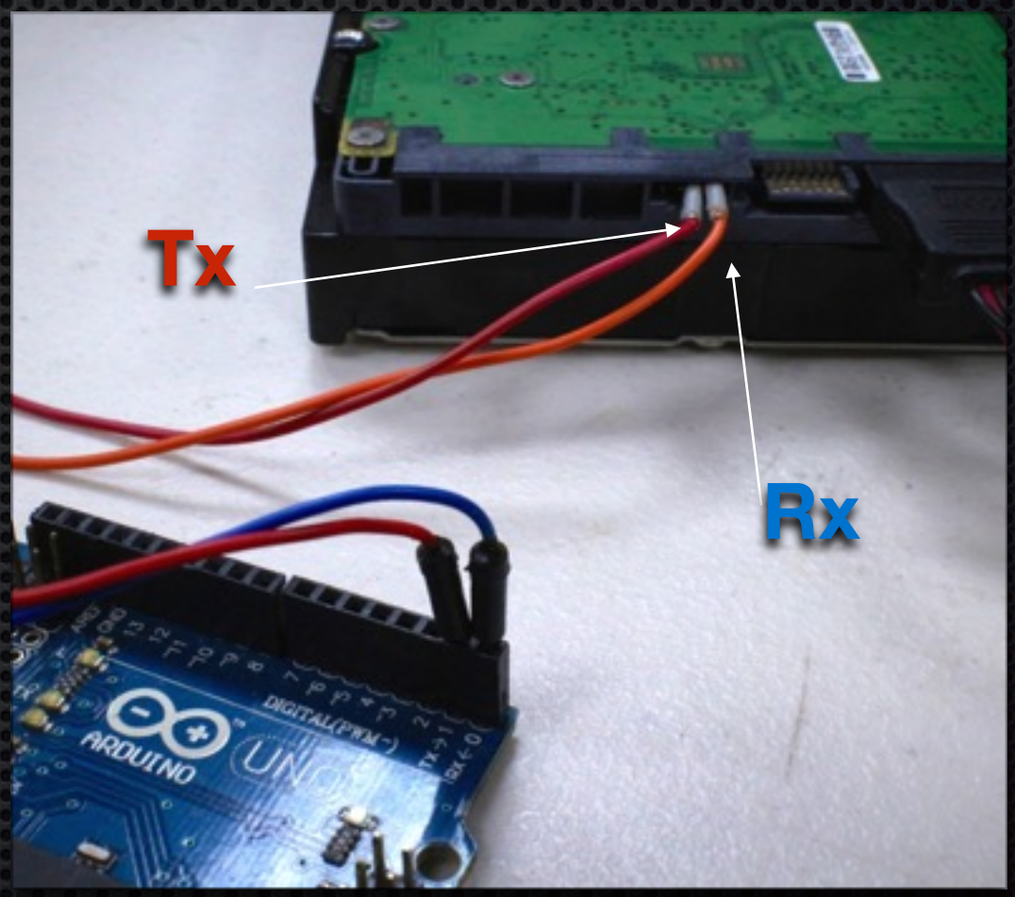
HDD TTL 串口指令

Apple EFI Passoword

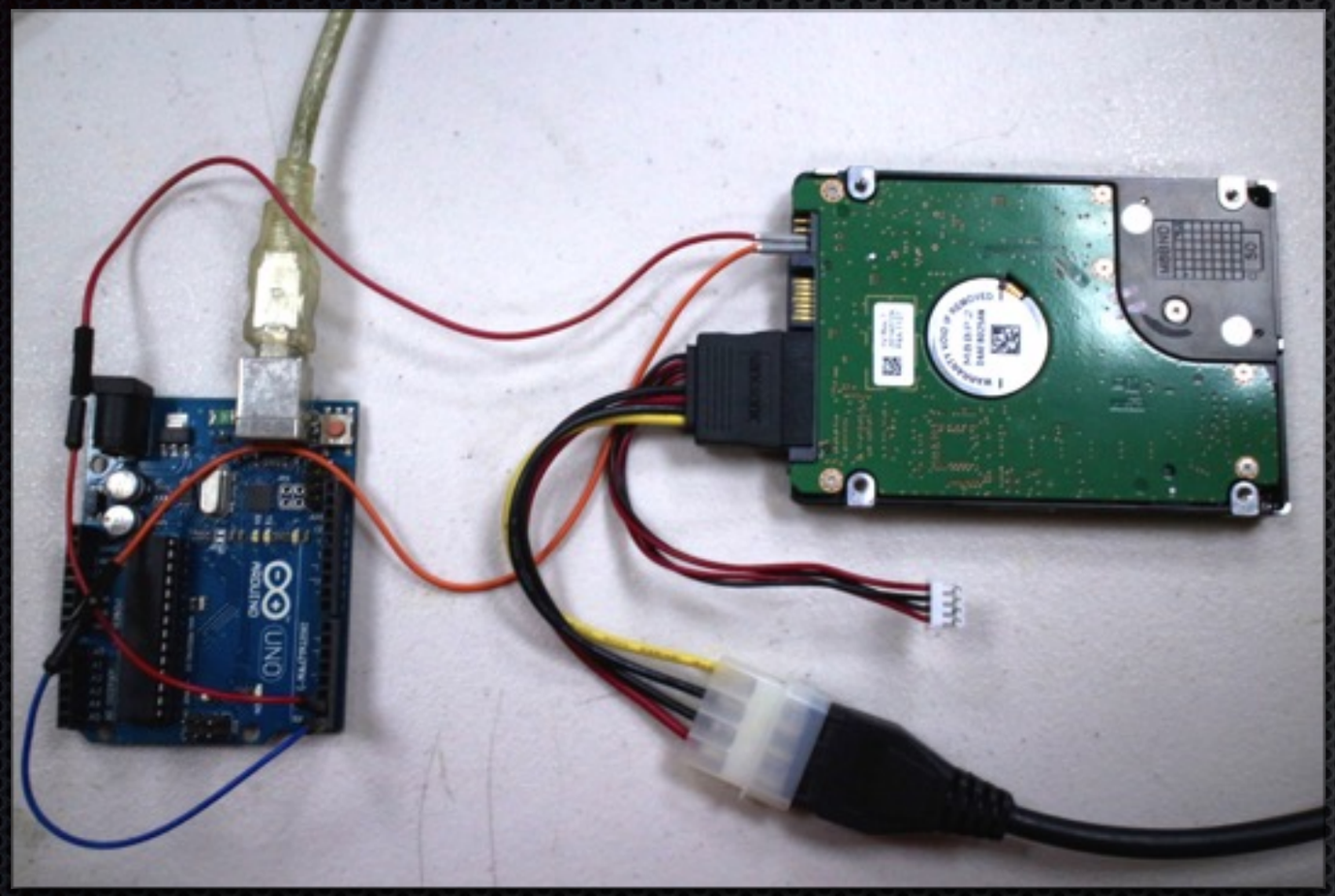
從應用中學習電子訊號原理

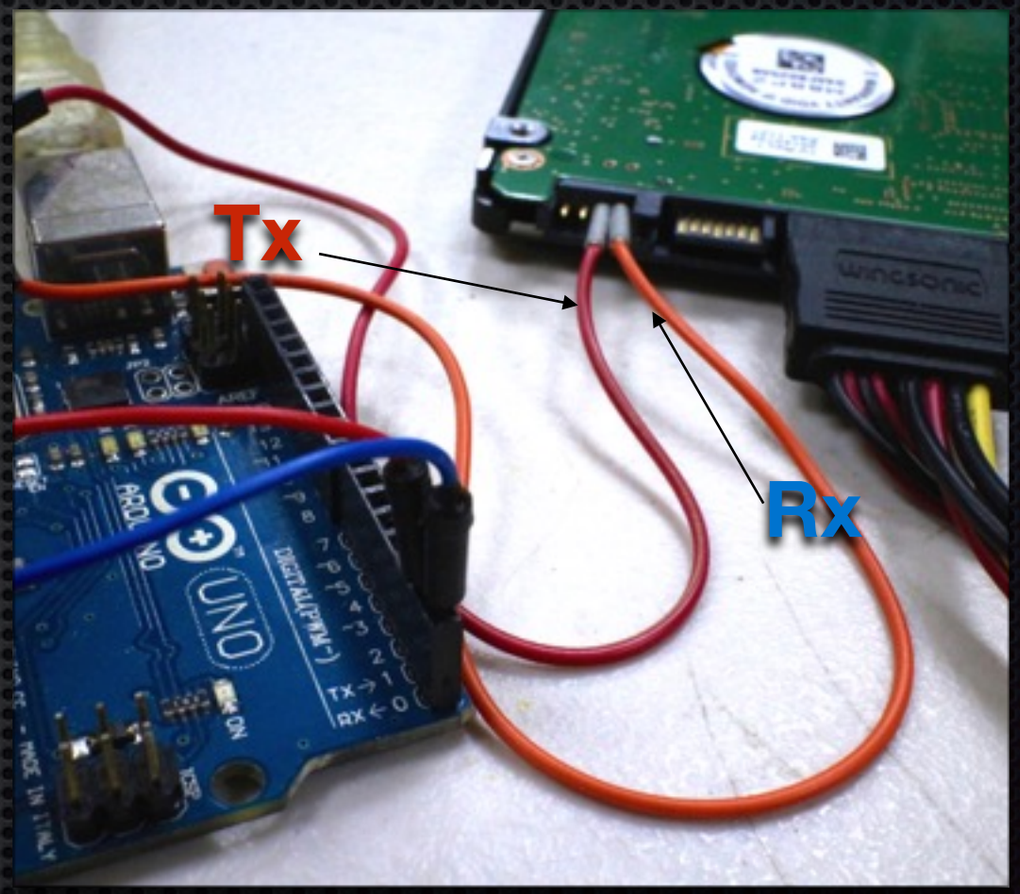
Seagate UART 接線法





Samsung UART 接線法





連接Seagate HDD 終端

```
screen /dev/tty.usbmodem1421 38400||
```

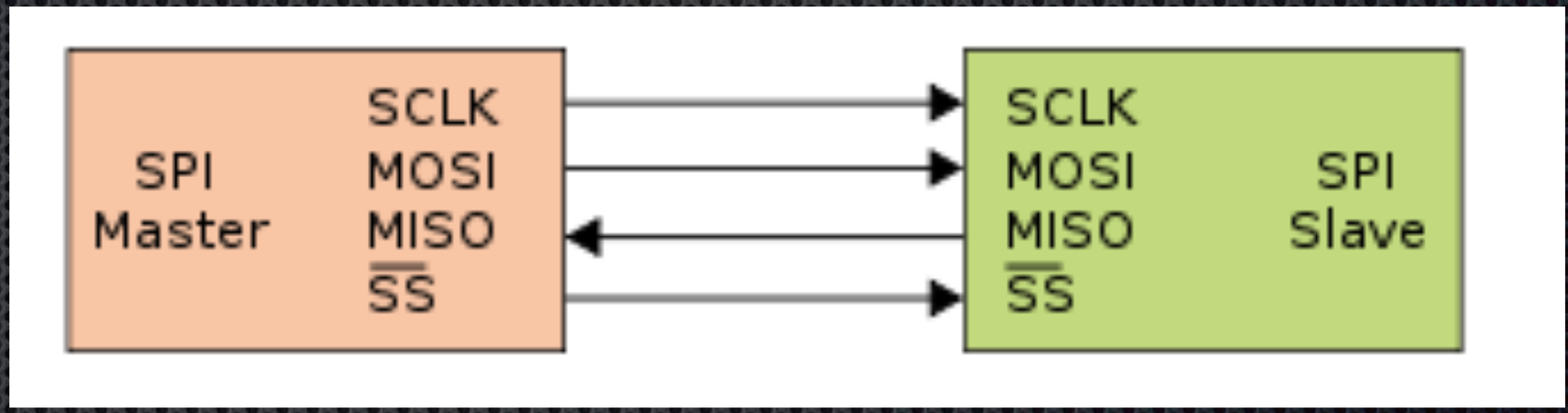
```
Rst 0x20M
(P) SATA Reset
 PASS
No Phy: Staggered spin bypass
```

Seagate 硬碟指令集

- 通病維修
- F3 C>Q (按下去後有指令說明)
  Online ^A: Rev 0002.0000, Flash, DisplayFirmwareRev
  Online ^B: Rev 0001.0000, Flash,
  GetThermistorTemperature
  Online ^C: Rev 0001.0000, Flash, FirmwareReset
  Online ^I: Rev 0001.0000, Flash, DisplayControllerRegs
  Online ^K: Rev 0001.0000, Flash, DisplayDstStatus
  Online ^L: Rev 0003.0000, Flash, DisplaySignOnMsg
  .....

SPI 協議

SPI是一種4線同步序列資料協定，串列外設介面
一般是4線，有時亦可為3線，可連接memory , RTC ,
ADC ,DAC ...etc



那些東西有用上SPI Flash?

- Router 你把bootloader 都刷掛了,就只能用spi 刷入
- 硬碟ROM
- 電腦主機版BIOS 內有密碼或序號....

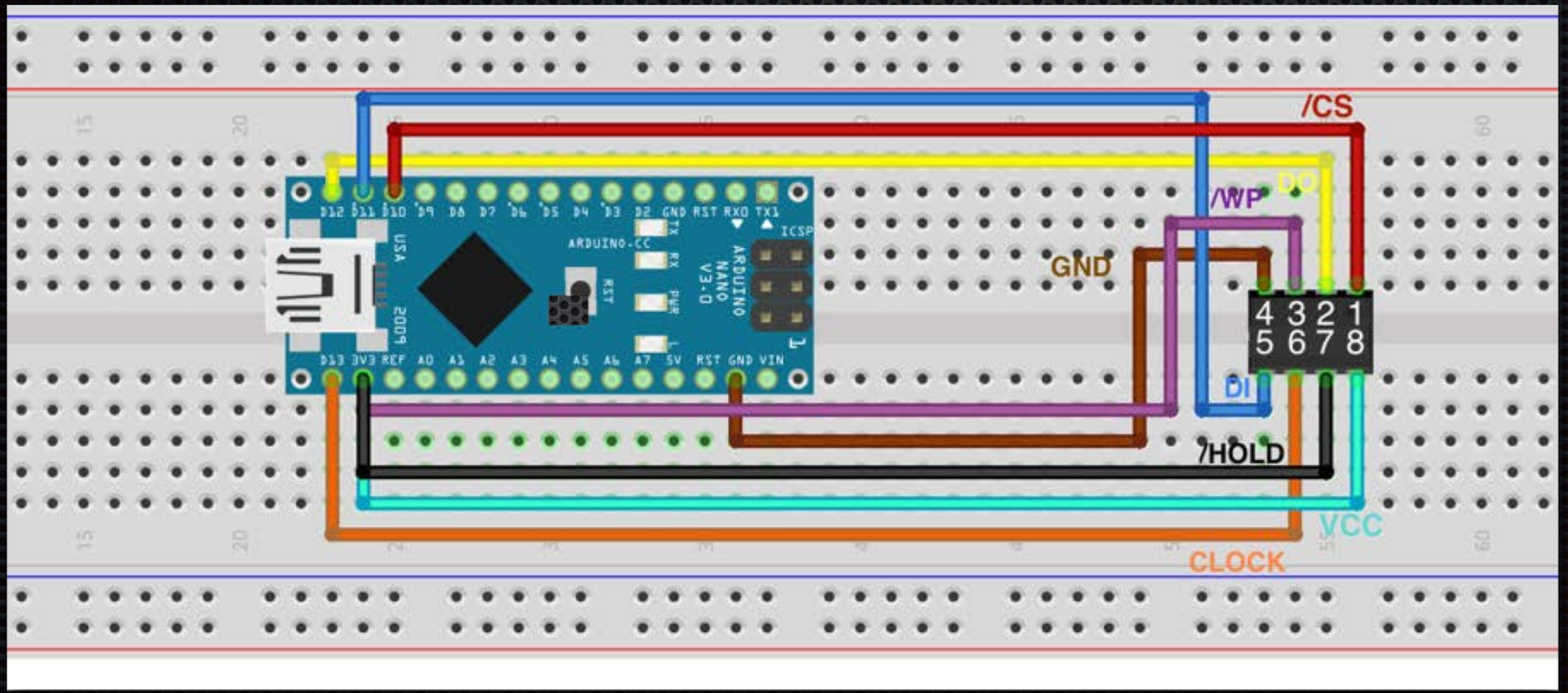
把Ardino 變成SPI 編程器

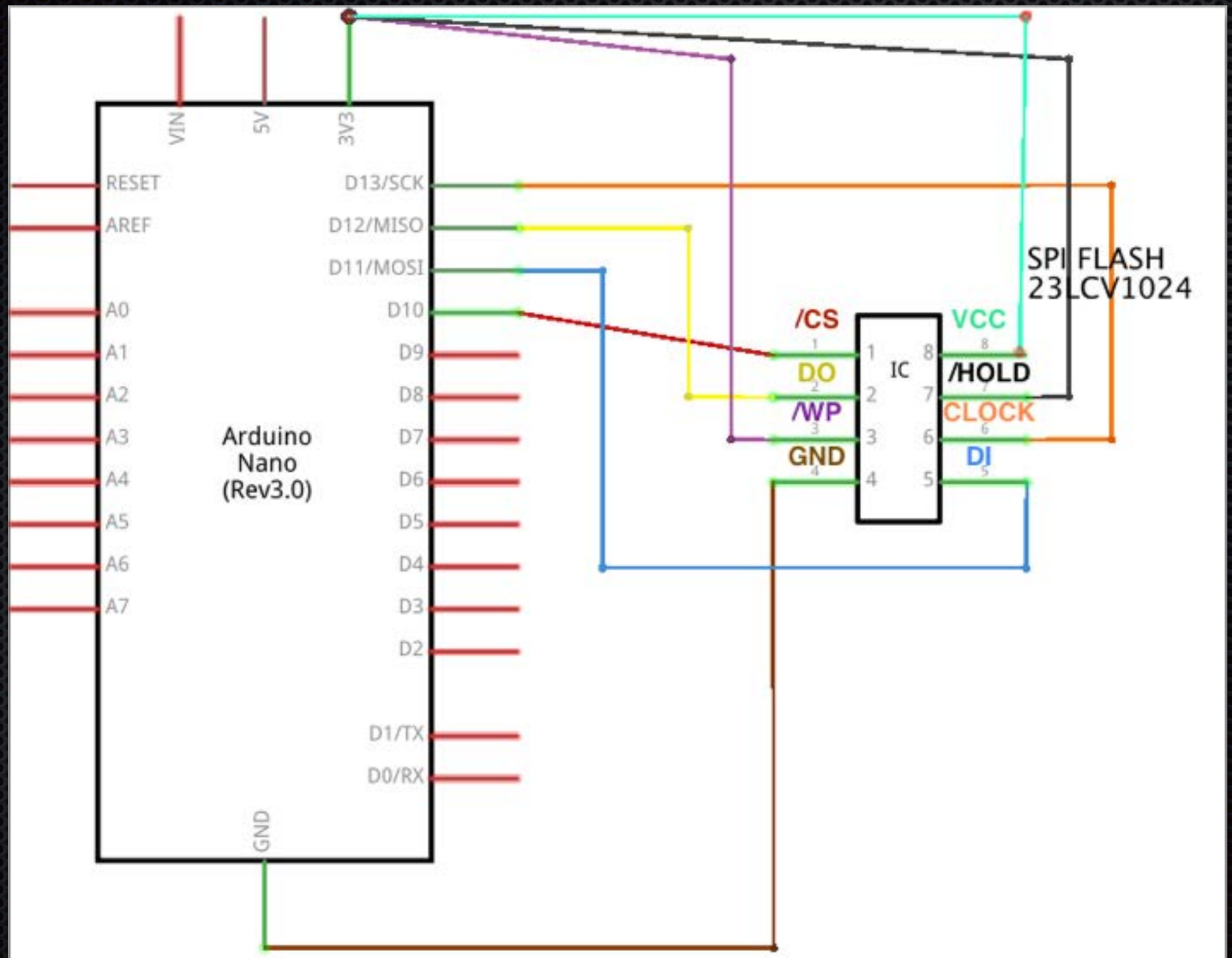
- 一般用的Arudino IDE 是以一個UI 包起 AVR Toolchian.
- SPI 編程器還要一些IC spec資料.因此不能單純做SPI 通訊
- 注意工作電壓 有分5V 跟 3.3V
  UNO 5V , Nano 3V ,5V 都可

CrossPack for AVR in OSX

- 下載網址：
  https://www.obdev.at/products/crosspack/download.html

Arduino 麵包板接法

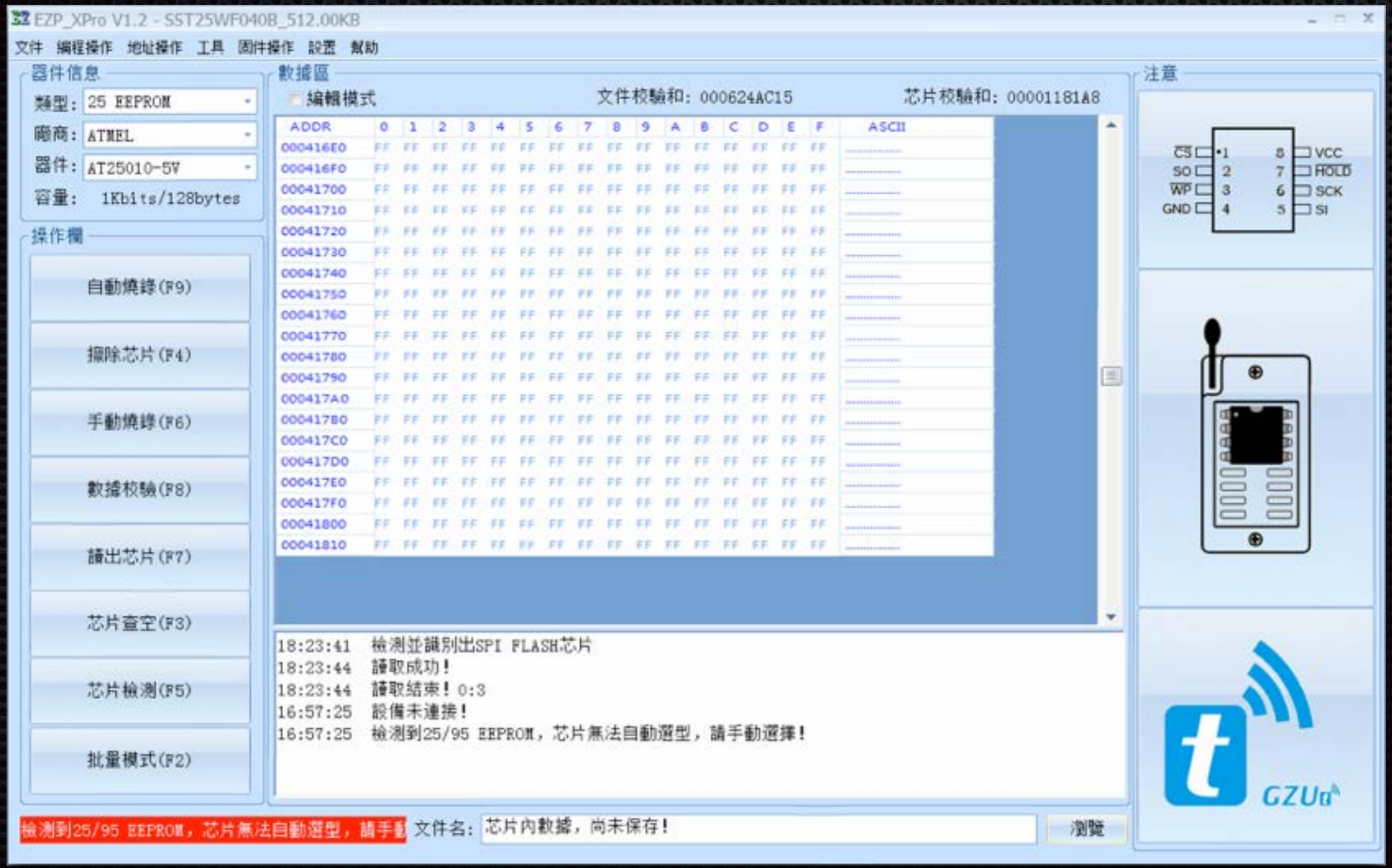



VIN
5V
3V3
RESET
AREF
A0
A1
A2
A3
A4
A5
A6
A7
D13/SCK
D12/MISO
D11/MOSI
D10
D9
D8
D7
D6
D5
D4
D3
D2
D1/TX
D0/RX
GND
Arduino
Nano
(Rev3.0)
SPI FLASH
23LCV1024
/CS
DO
/WP
GND
VCC
/HOLD
CLOCK
DI
IC

拿Arduino 做SPI編程器 軟體

- http://flashrom.org/Serprog/Arduino_flasher 去 git吧
- 燒錄Arduino 程式碼
  make u2
- Dump ROM
  flashrom -p serprog:dev=/dev/ttyUSB0:2000000

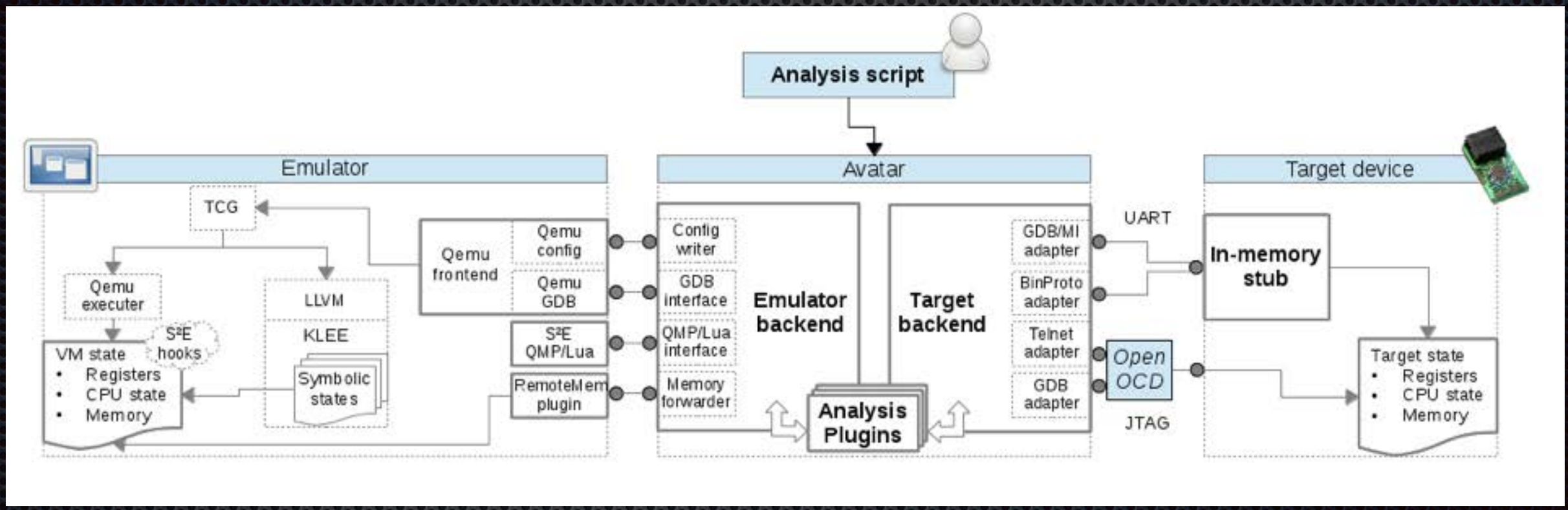
SPI IC 燒錄器


EZP_XPro V1.2 - SST25WF040B_512.00KB
文件 編程操作 地址操作 工具 固件操作 設置 幫助
器件信息
類型: 25 EEPROM
廠商: ATMEL
器件: AT25010-5V
容量: 1Kbits/128bytes
操作欄
自動燒錄(F9)
擦除芯片(F4)
手動燒錄(F6)
數據校驗(F8)
讀出芯片(F7)
芯片查空(F3)
芯片檢測(F5)
批量模式(F2)
數據區
編輯模式
文件校驗和: 000624AC15
芯片校驗和: 00001181A8
ADDR 0 1 2 3 4 5 6 7 8 9 A B C D E F ASCII
000416E0
000416F0
00041700
00041710
00041720
00041730
00041740
00041750
00041760
00041770
00041780
00041790
000417A0
000417B0
000417C0
000417D0
000417E0
000417F0
00041800
00041810
18:23:41 檢測並識別出SPI FLASH芯片
18:23:44 讀取成功!
18:23:44 讀取結束! 0:3
16:57:25 設備未連接!
16:57:25 檢測到25/95 EEPROM，芯片無法自動選型，請手動選擇!
檢測到25/95 EEPROM，芯片無法自動選型，請手動
文件名: 芯片內數據，尚未保存!
瀏覽
注意
CS 1
SO 2
WP 3
GND 4
8 VCC
7 HOLD
6 SCK
5 SI
GZUt

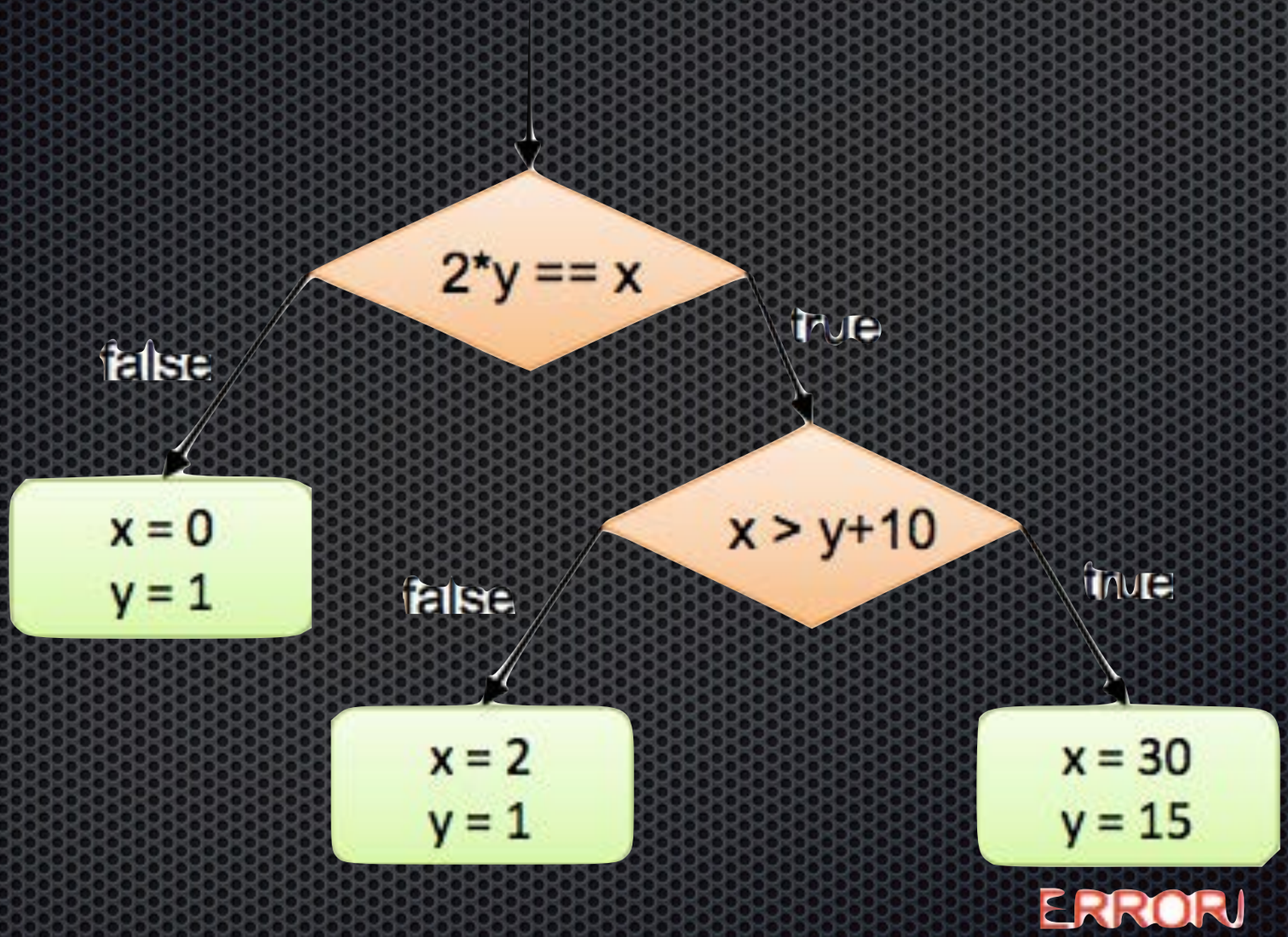
逆向當代封閉嵌入式系統的問題

- 沒有原始碼 只有binary 韌體
- 沒有 toolchain
- 沒有文件
- 只能用封閉Debug或燒錄軟硬體工具（如高通QPST）

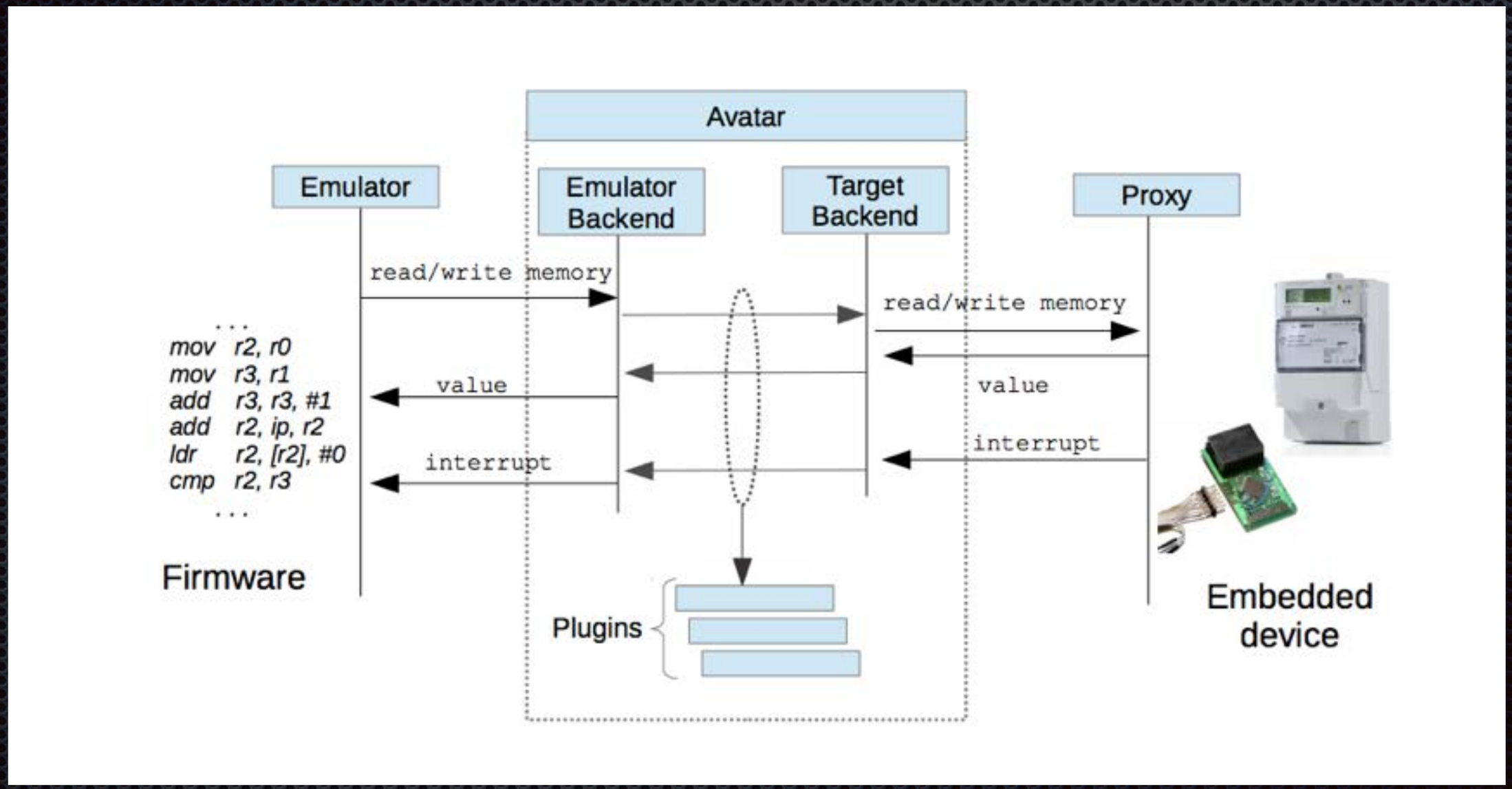
“真”外星逆向技術 Avatar 專案



Symbolic Execution（符號執行)



Avatar 提供的Bridge



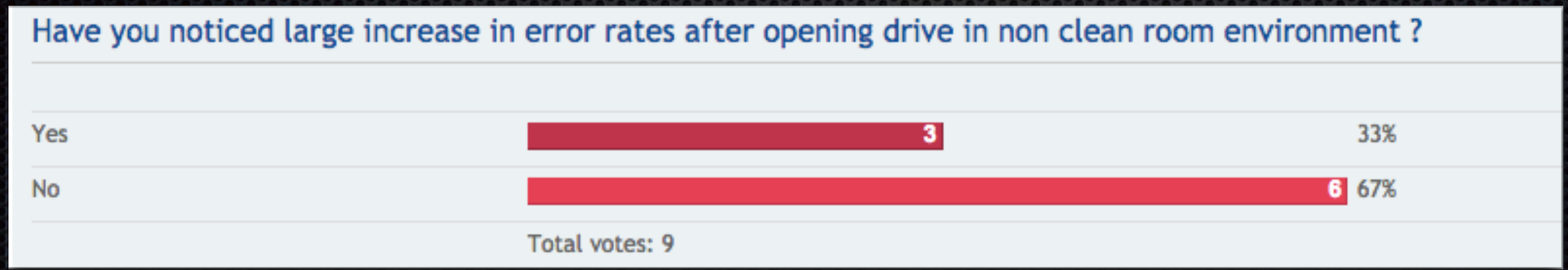
整個 Symbolic Execution逆向架構

- S²E (Qemu +Qemu LLVM +Klee)
  模擬ARM and symbolic execution
- GDB and OpenOCD
  做目標物通訊 (UART 或JTAG)
- Avatar
- 逆向分析工具 IDA Pro

逆向Seagate HDD成果

- 拆解Segate Update FW結構
- 可用於維修硬碟韌體

超潔淨無塵室真的有用嗎？？



- 資料來源：全球最專業硬碟論壇
  http://malthus.mooo.com/viewtopic.php?t=20&start=20

材料多好像比教實用?

其實DR 專家還是做好 Program Kiddie

- 材料相容性經驗
- 更換材料穩定性
- 熟知硬碟工作原理
- 狀況問題與解決經驗
- 自我不斷學習

技術上的結論

- 硬碟是很有趣的學習 embedded security
- 未來市場主流的SSD 用的技術一樣脫離不了 ATA Command,UART .

行業的結論

- 資訊越來越開放,讓消費者瞭解成本與風險,而不是在於過度吹噓
- 行業要有工會跟制度避免惡性破壞客戶數據
- 合理的處理客戶案件 ,確實幫客戶處理,並不只搶完低難度的.

朝聞道 夕可死矣

- 一路摸索 跌跌撞撞 要感謝很多人