

解析

儲存embedded架構原理實現漏洞與反制



前言

傳台灣某公司主控 SSD 藏後門，"銀監會要求調查"

這是真實的嗎？

儲存裝置有後門嗎？

如果有，哪又是怎樣的狀況，我們要怎樣防範？

講師介紹

Thx

Hitch 2015 ,2012 講師
工信部高級資料恢復工程師
ACELab Raid ,Flash 認證
OSSLab 開放軟體實驗室創辦人



儲存裝置上的嵌入式架構

CPU Core + RAM

ROM

碟片上的韌體架構



硬碟載入 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

WD 模块列表

The screenshot displays the WD software interface with the following components:

- Header:** "Mrt - [ATA1 - WDC Maxwell]"
- Menu Bar:** MRT应用(F), 帮助(H), 设备区操作(S), 工具(T), 窗口(W), 帮助(H)
- Toolbar:** Contains various icons for navigation and operations.
- Device Information:**
 - 型号: ADC WD5000AELS-2297BJ
 - 序列号: AD-WLAS1114341
 - 固件版本: J1.03B01
 - 容量: 316773168 (465.76 GB)
- Other Information:**
 - 品牌: Atlantis
 - SA Cyl: 170 Head: 4 SPT: 13:1
 - ROM版本: U2.38C
 - 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	重复级别	长度(扇区)	说明	读	写	校验
00C1	B	C018	Modules directory			
0026	Dd	000A	SA Defects			
00C1	Dr	C001	Calibrations module			
00C3	Dd	C39E	P-List (Primary defect...			
0051	Ad	C255	Transistor			
000C	B	C005	Models table			
0024	C	C017	G-List (Grown defect ...			
0032	Ad	C020	Relo Bad Block Module			
0036	Ad	C009	I-List Module			
0029	B	C006	microprogram code			
0040	As	C07D	Adaptive data			
0041	As	C07D	Adaptive data			
0042	As	C07D	Adaptive data			
0043	As	C07D	Adaptive data			
004E	B	C01C	microprogram code			
0049	As	C003	Adaptive data			
004A	As	C018	Adaptive data			
004D	As	C001	Adaptive data			
00C3	As	C01C	Format Select Data Ma...			
00C4		C311	Family models configura...			
0025		C101				
- Bottom Panel:**
 - 日志: ROM对象, 模块对象
 - Power: ON
 - Status (ATA1): ESY, EDC, DV7, DSC, DRQ, CRR, IDR, ERR
 - Error: BDX, URC, INF, ADR, ION, ADN
- Taskbar:** Shows system icons, taskbar icons (including MRT), and system clock (11:23, 2015/7/21).

硬碟embeddedsystem 架構

- 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—丟失 資料—去不復返**

中斷硬碟啟動流程

硬碟安全系統正常啟動 就會進入 安全系統鎖住硬碟
韌體損壞硬碟則是載入錯誤韌體到一半,造成硬碟本體當
機.

因此 打斷正常啟動流程
可用於破解儲存安全保護與資料救援嚴重損壞韌體

ATA Vendor-specific command (工廠指令集)

公開的T10 文件就有說明

Something (e.g., a bit, field, or code value) that is not defined by the standard and may be used differently in various implementations.

讀寫韌體,ROM操作等特別操作就要用工廠指令集
工廠指令集的原由:生產與維修

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							

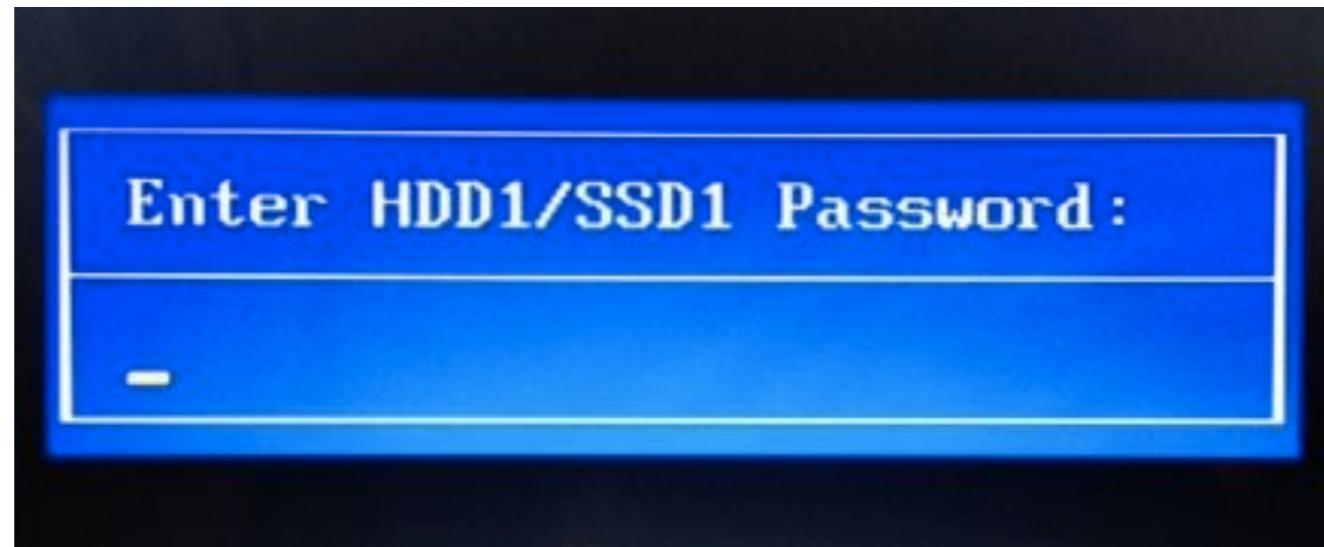
儲存裝置安全保護

ATA 保護

AES 加密

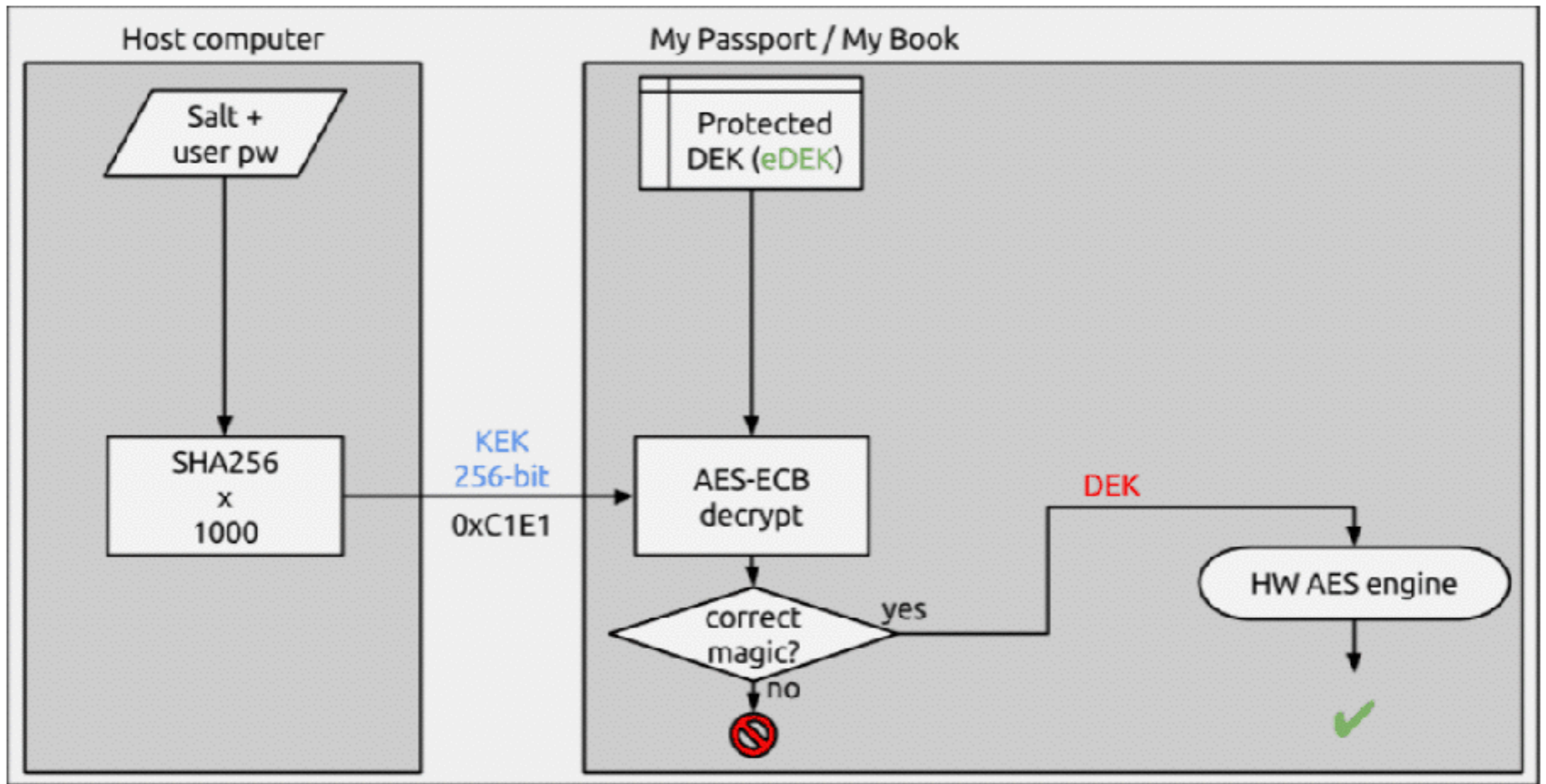
韌體 保護

ATA 加密



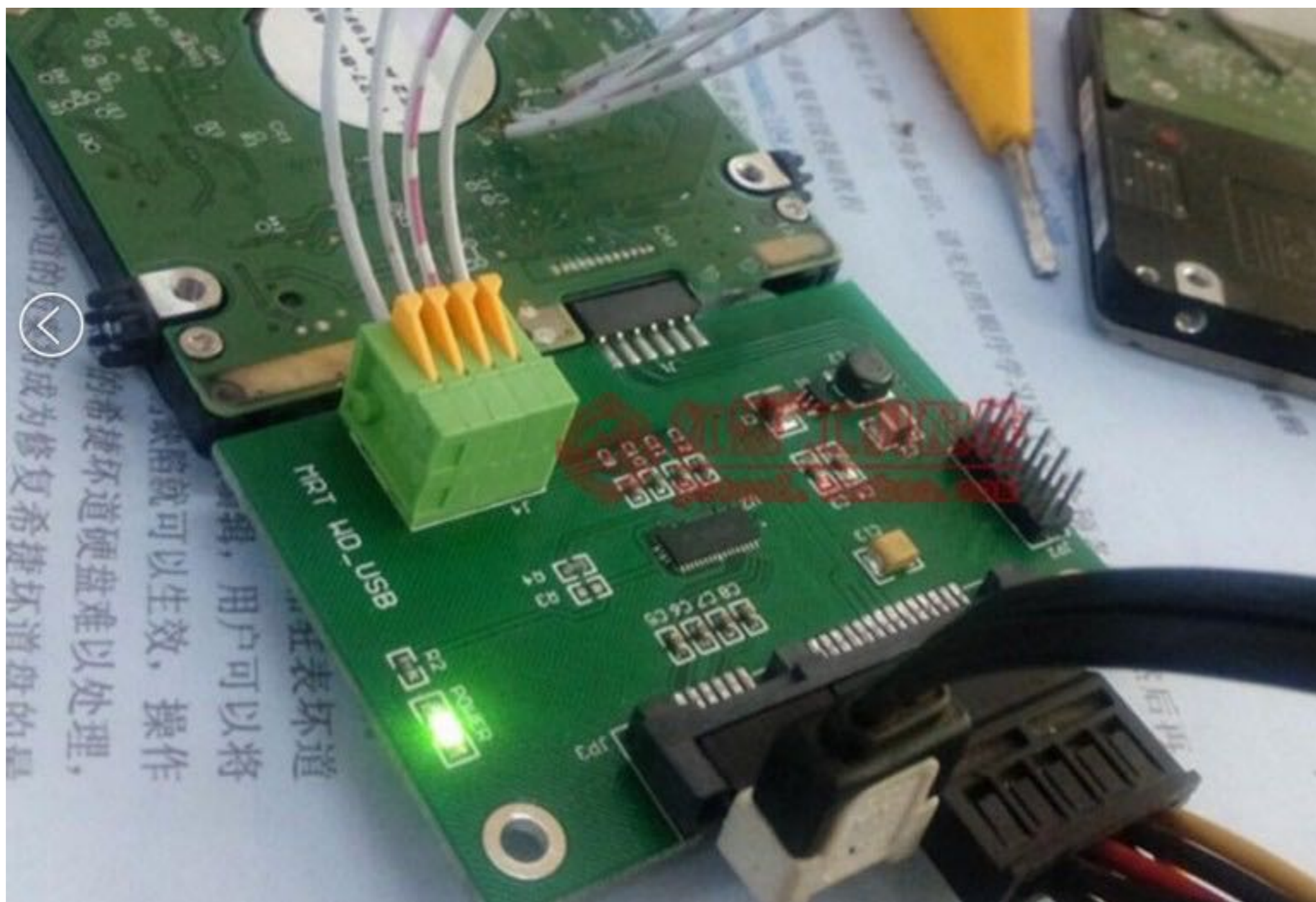


AES 加密

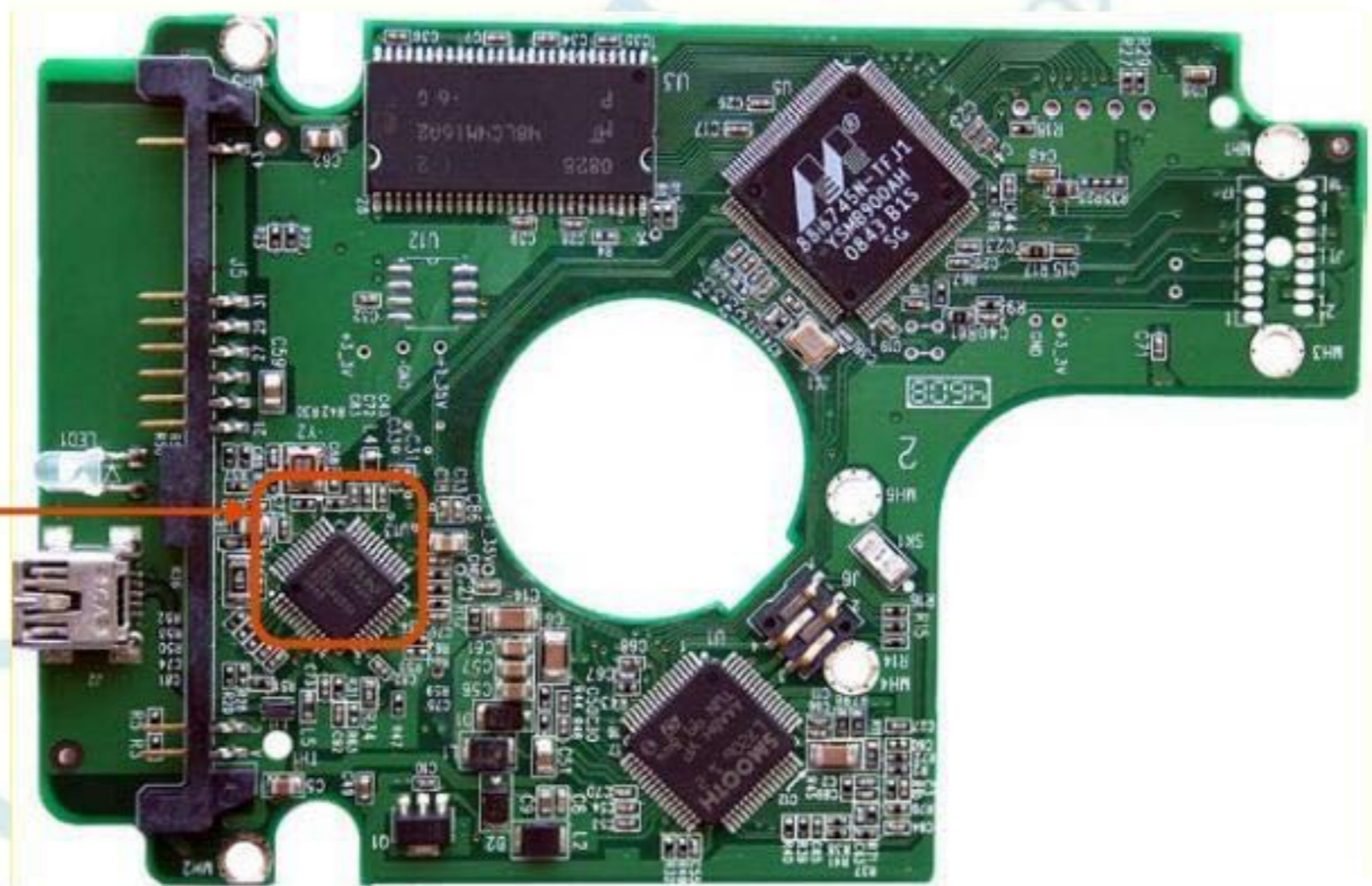






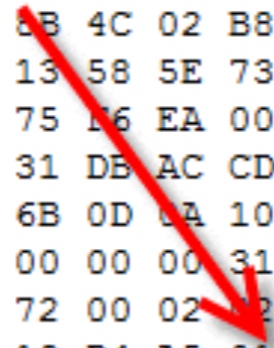


USB<->SATA МОСТ



Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F		
00000000	FC	31	C0	8E	D0	31	E4	8E	D8	8E	C0	BE	00	7C	BF	00	ü1ÀŽĐ1äŽØŽÀ% . ç.	
00000010	06	B9	00	01	F3	A5	BE	EE	07	B0	08	EA	20	06	00	00	.²..ó%í.°.ê ...	
00000020	80	3E	B3	07	FF	75	04	88	16	B3	07	80	3C	00	74	04	€>³.ÿu.^.³.€<.t.	
00000030	08	06	AF	07	83	EE	10	D0	E8	73	F0	90	90	90	90	90	..̄.fi.Đèsø.....	
00000040	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	
00000050	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	
00000060	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	
00000070	90	90	90	90	90	90	90	90	90	90	90	90	90	90	BE	BE%%	
00000080	07	B0	00	B9	04	00	80	3C	00	75	6E	FE	C0	83	C6	10	.°.²..€<.unpÀfE.	
00000090	E2	F4	31	DB	B4	0E	BE	9D	07	8A	0E	AF	07	AC	D0	E9	âô1Û'.%..Š.̄.-Đé	
000000A0	73	02	CD	10	08	C9	75	F5	B0	3A	CD	10	31	C0	CD	16	s.Í..Éuø°:Í.1ÀÍ.	
000000B0	3C	00	74	F8	BE	8B	07	B9	02	00	E8	BA	00	3C	0D	74	<.tø%«.²..è°.<.t	
000000C0	B4	3C	61	72	06	3C	7A	77	02	2C	20	88	C3	BE	9D	07	'<ar.<zw., ^Ä%..	
000000D0	8A	0E	AF	07	AC	D0	E9	73	04	38	C3	74	06	08	C9	75	Š.̄.-Đés.8Ät..Éu	
000000E0	F3	EB	AF	B8	0D	0E	31	DB	CD	10	8D	84	62	00	3C	07	óë̄,..1ÛÍ...„b.<.	
000000F0	75	07	B0	1F	A2	AF	07	EB	99	31	D2	B9	01	00	3C	04	u.°.c̄.ë™1ò²..<.	
00000100	74	11	73	F3	30	E4	B1	04	D2	E0	BE	BE	07	01	C6	8A	t.só0ä±.Òà%%.EŠ	
00000110	16	B3	07	BF	05	00	56	F6	C2	80	74	31	B4	41	BB	AA	.³.ç..VöÄ€t1'A»²	
00000120	55	52	CD	13	5A	5E	56	72	1F	81	FB	55	AA	75	18	F6	URÍ.Z^Vr..ûUªu.ö	
00000130	C1	01	74	13	8B	44	08	8B	5C	0A	BE	8D	07	89	44	08	Á.t.<D.<\.%..%D.	
00000140	89	5C	0A	B4	42	EB	0C	8A	74	01	8B	4C	02	B8	01	02	%\.'Bë.Št.<L.,..	
00000150	BB	00	7C	50	C6	06	8F	07	01	CD	13	58	5E	73	05	4F	». PÆ....Í.X^s.O	
00000160	75	B4	EB	93	81	3E	FE	7D	55	AA	75	16	EA	00	7C	00	u'ë™.>p}Uªuöê. .	
00000170	00	BE	83	07	B9	0A	00	50	B4	0E	31	DB	AC	CD	10	E2	.%f.²..P'.1Û-Í.â	
00000180	FB	58	C3	54	65	73	74	44	69	73	6B	0D	0A	10	00	01	ûXÄTestDisk.....	
00000190	00	00	7C	00	00	00	00	00	00	00	00	00	00	31	32	33123	
000001A0	34	46	00	00	41	4E	44	54	6D	62	72	00	02	02	02	1F	4F..ANDTmbr.....	
000001B0	C7	00	00	80	00	00	00	00	19	D4	19	D4	A5	01	00	01	Ç..€.....Ô.Ô%...	
000001C0	01	00	07	FE	FF	99	3F	00	00	00	DB	02	E2	00	00	00	...pÿ™?...Û.â...	
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AAUª

Partition table





W D A E S

暴力破解

我在路上撿到工廠指令手冊



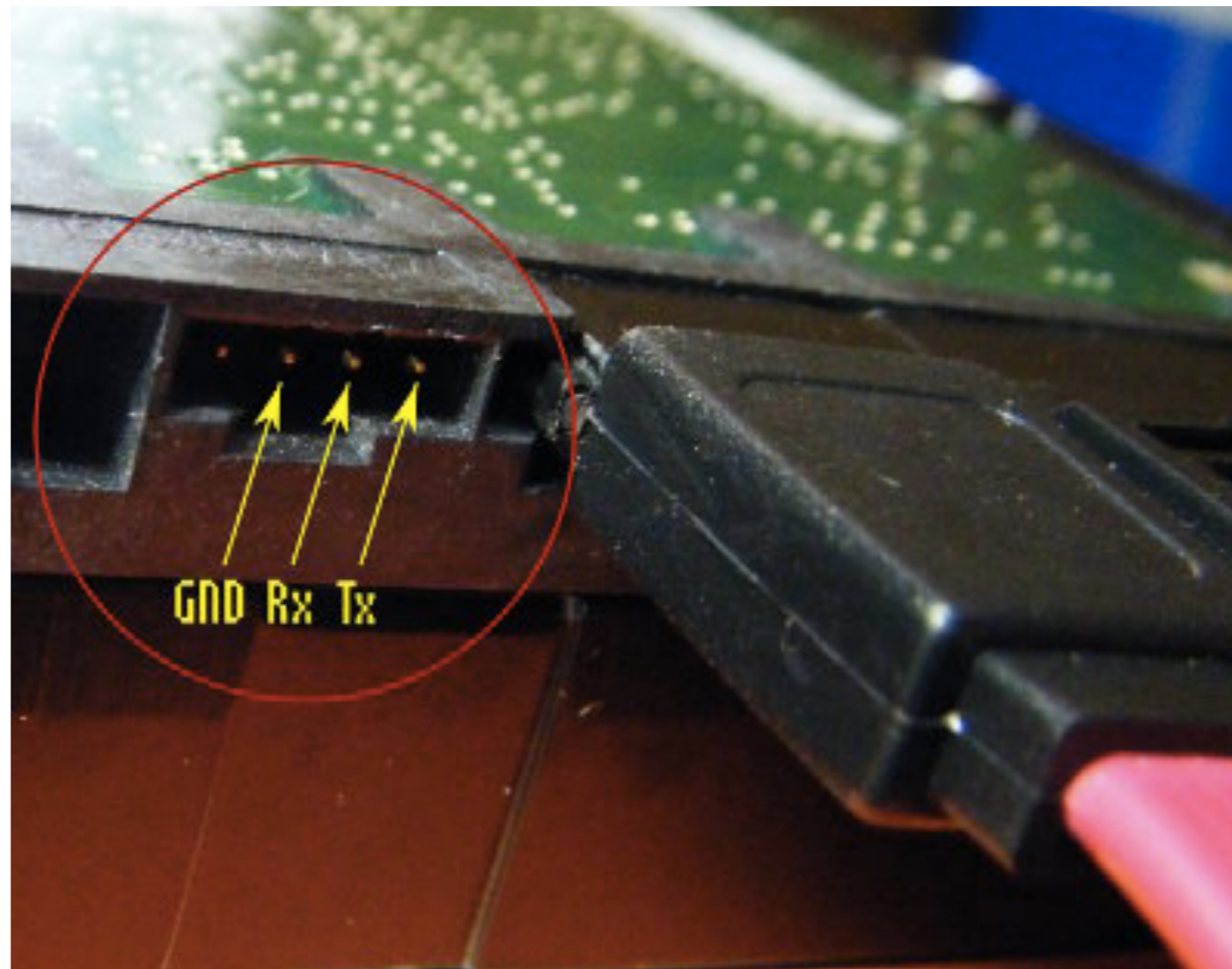
請你跟我這樣做(一)

Seagate F3 Serial Port Diagnostics

F3 串行端口诊断命令 中文翻译

(Rev.TR30)

請你跟我這樣做(二)

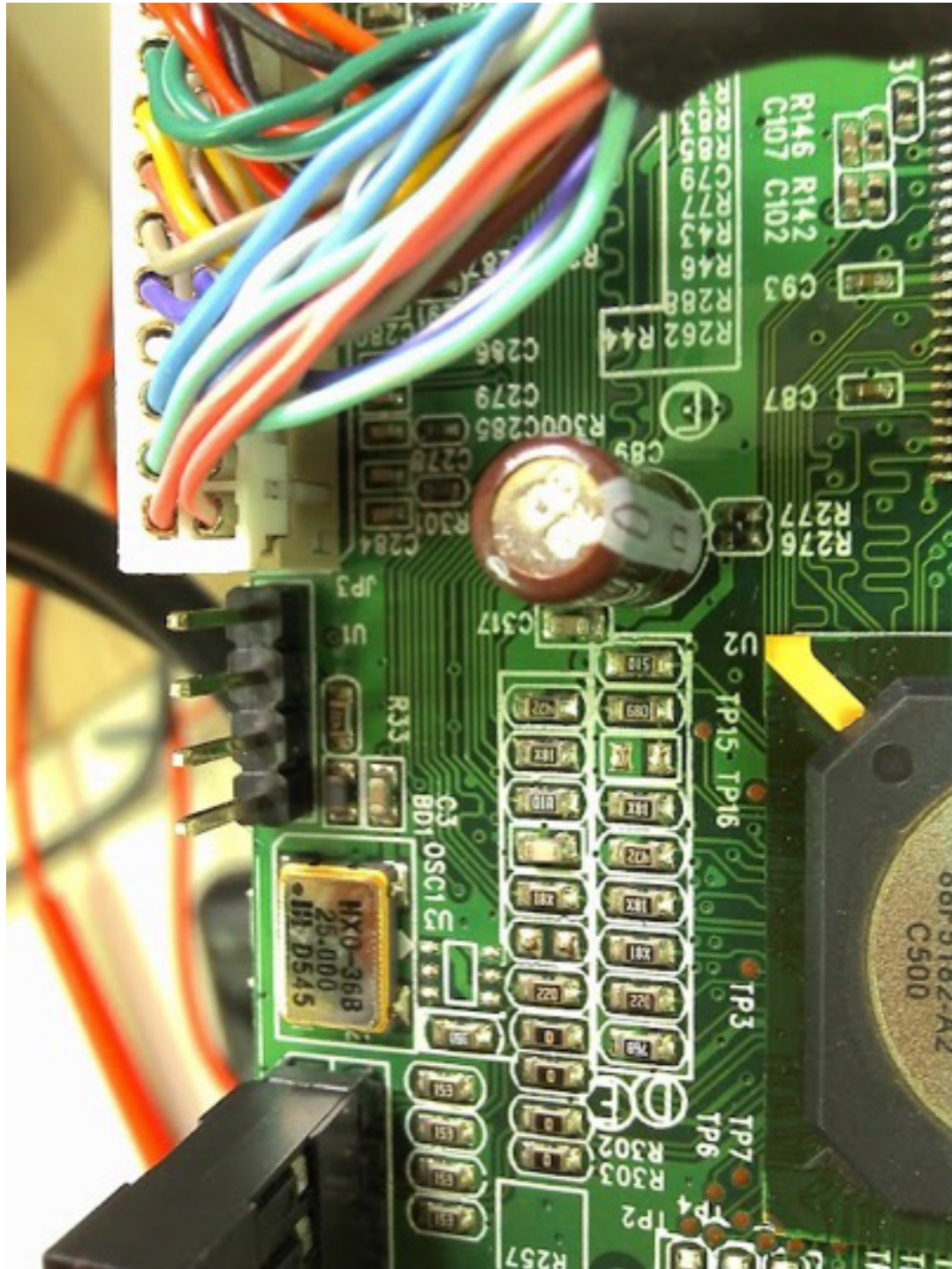


Serial TTL (UART)通訊

- 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)2.00mm, 4P排座
 - USB to TTL板 (拿Arduino也可替代)



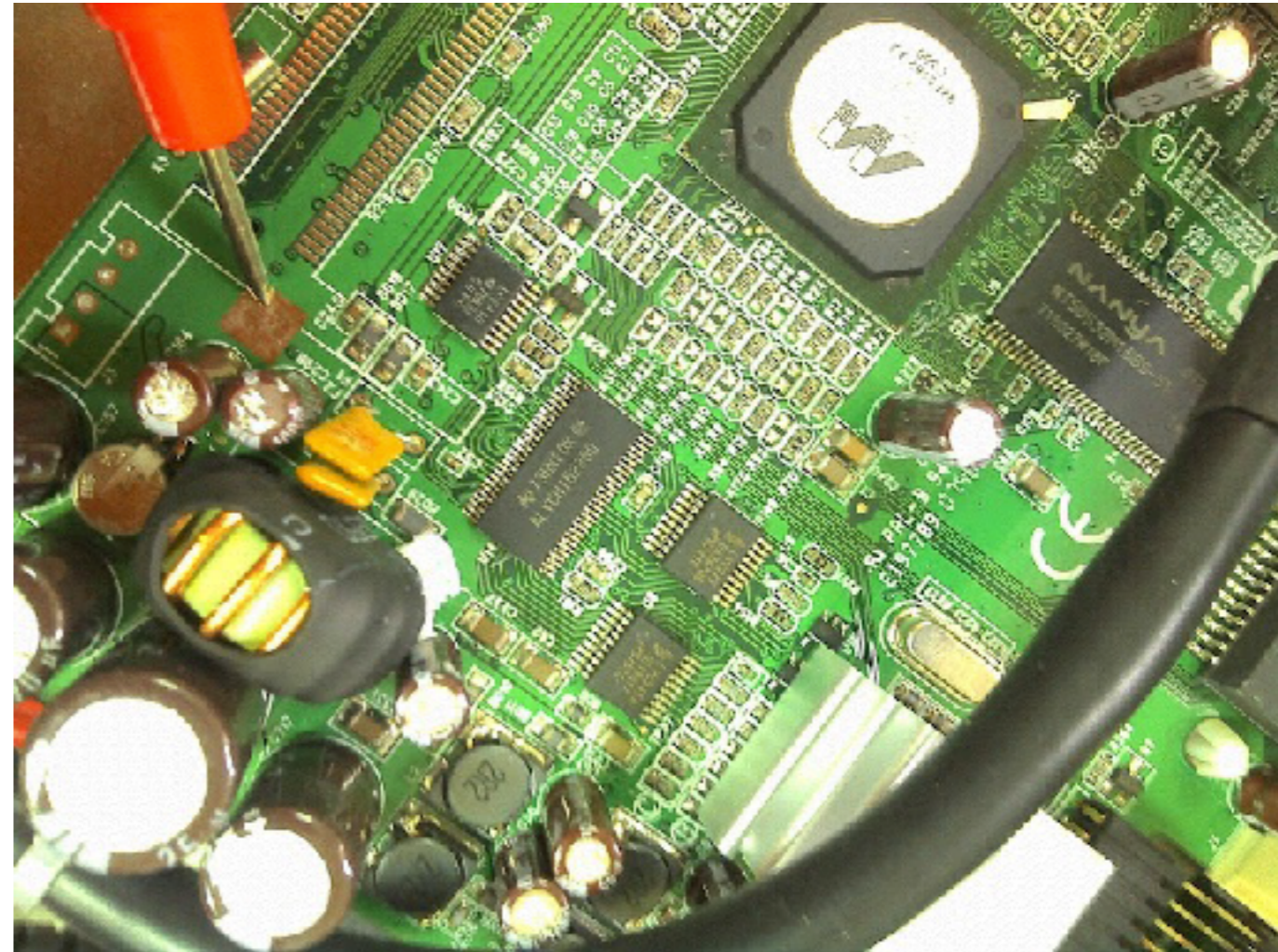
逆向Serial UART腳位



- 以一台ARM NAS
做範例

GND腳位判定

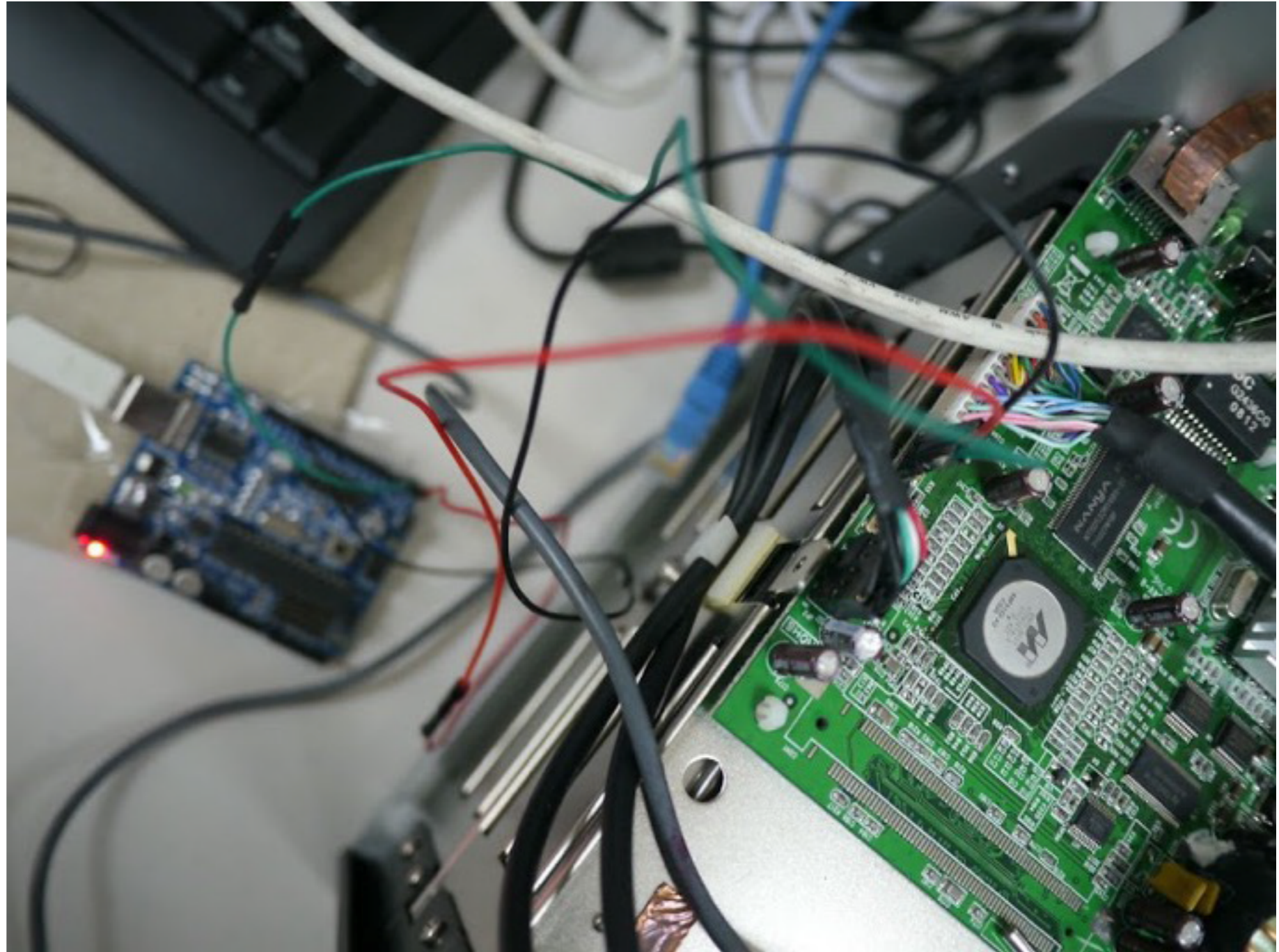
- 最好抓的是GND
- 先將embedded system斷電
GND一是大塊金屬點 或是電源座負極. 會導通 數位型三用電表轉到二極體測試檔位(可做導通測試有通會發聲)
- 另外一邊探針 則每個Pin都試, 發現第一根有跟接地點導通, 會翁鳴。
因此第一根為**GND**



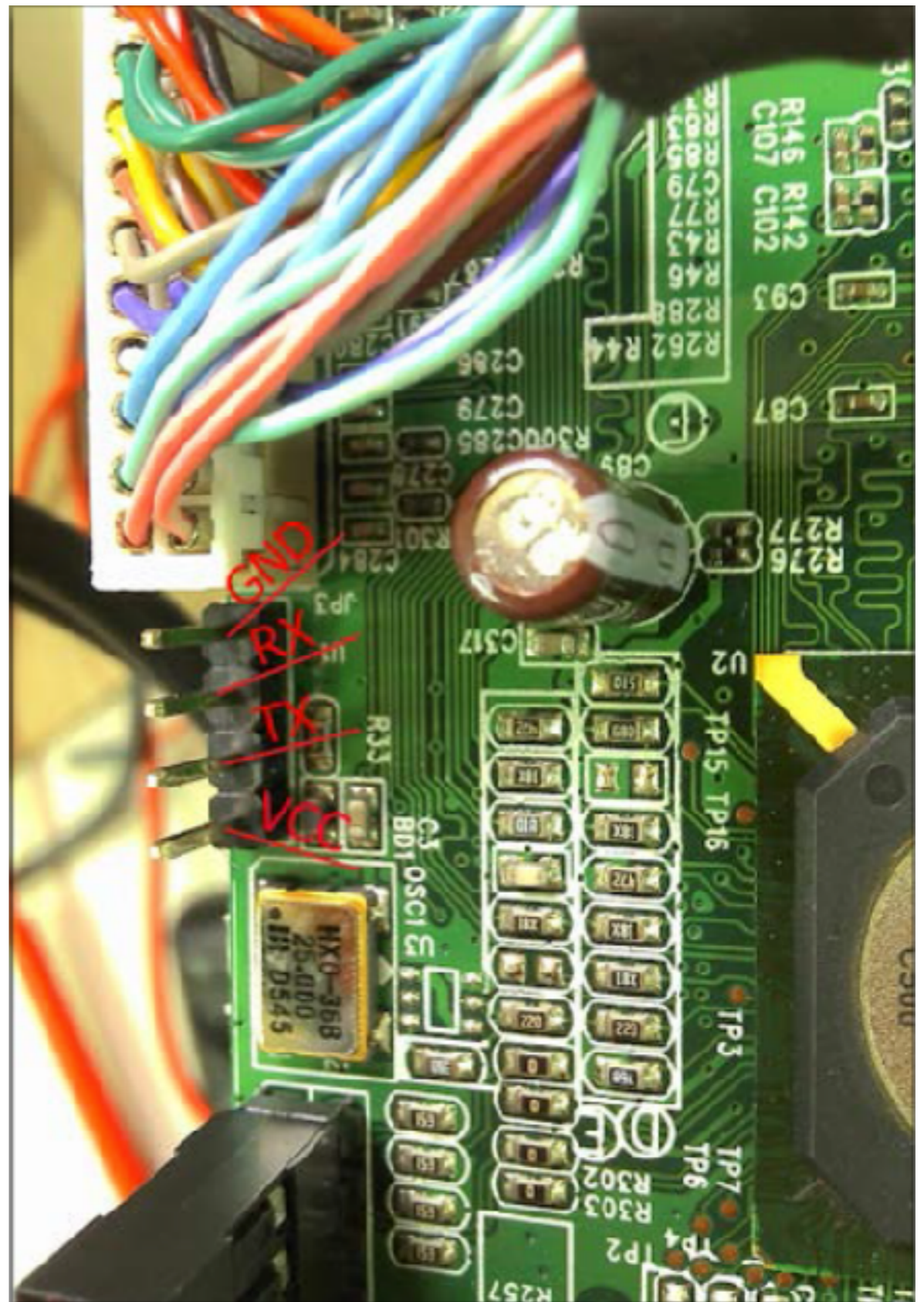
- 這時embedded system 再通電
把探針一根固定放 GND 測試每根與第一根已知 (GND)
相通電呀 發現當 1,4 腳位通電時3.3V或5V



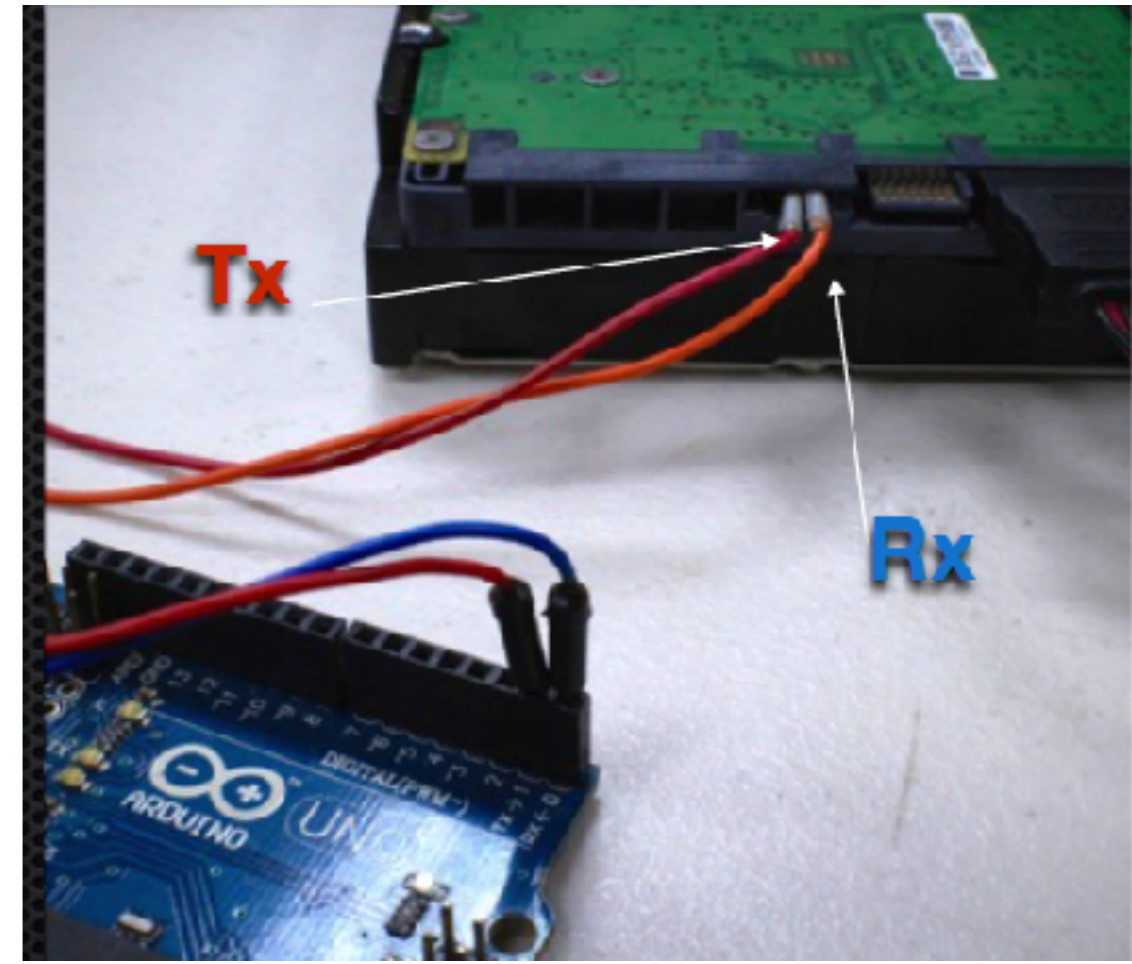
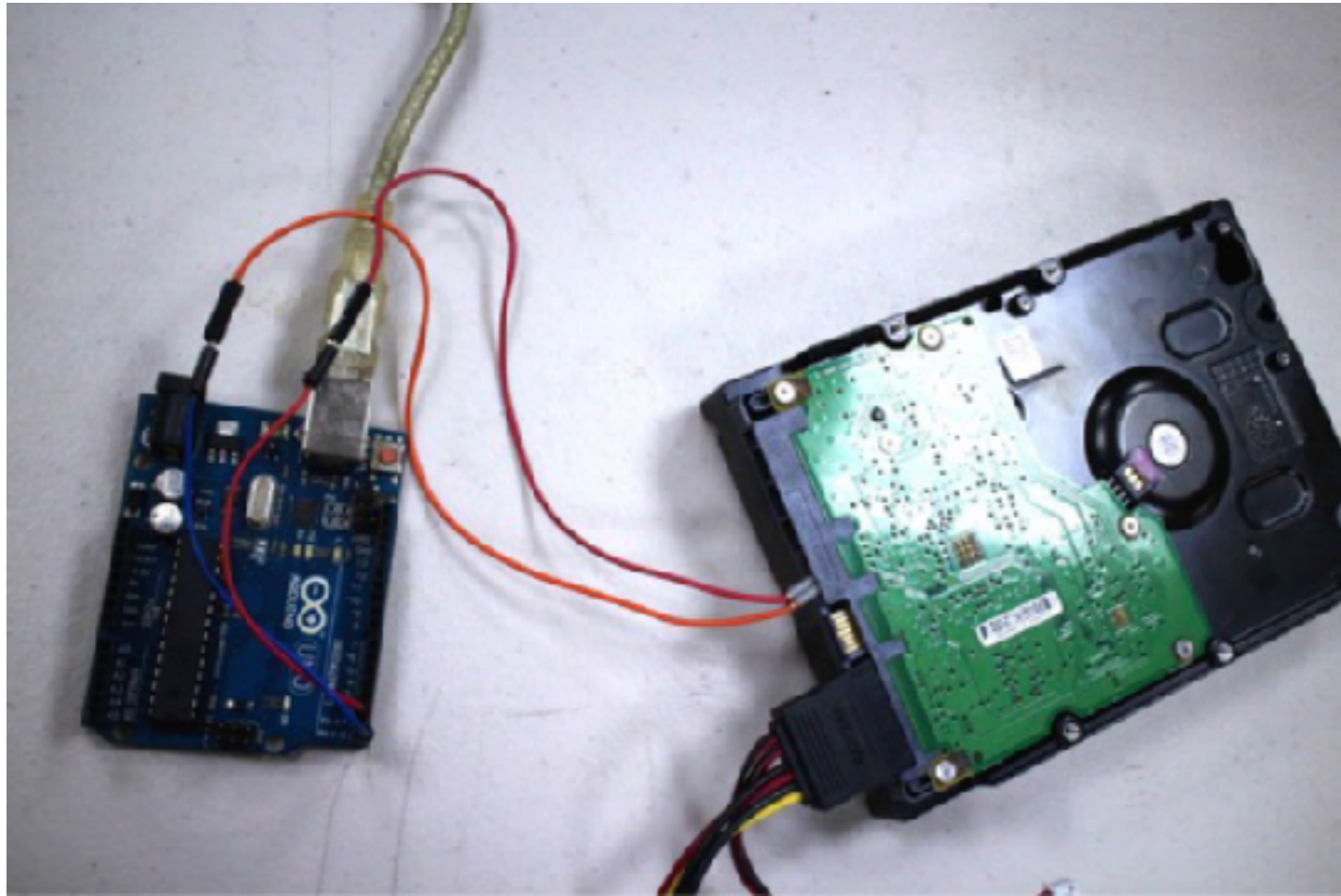
- 表示第四根為 VCC 。 RX TX , 就為中間二根。先顯示有字串再調速度用2400~115200 慢慢試



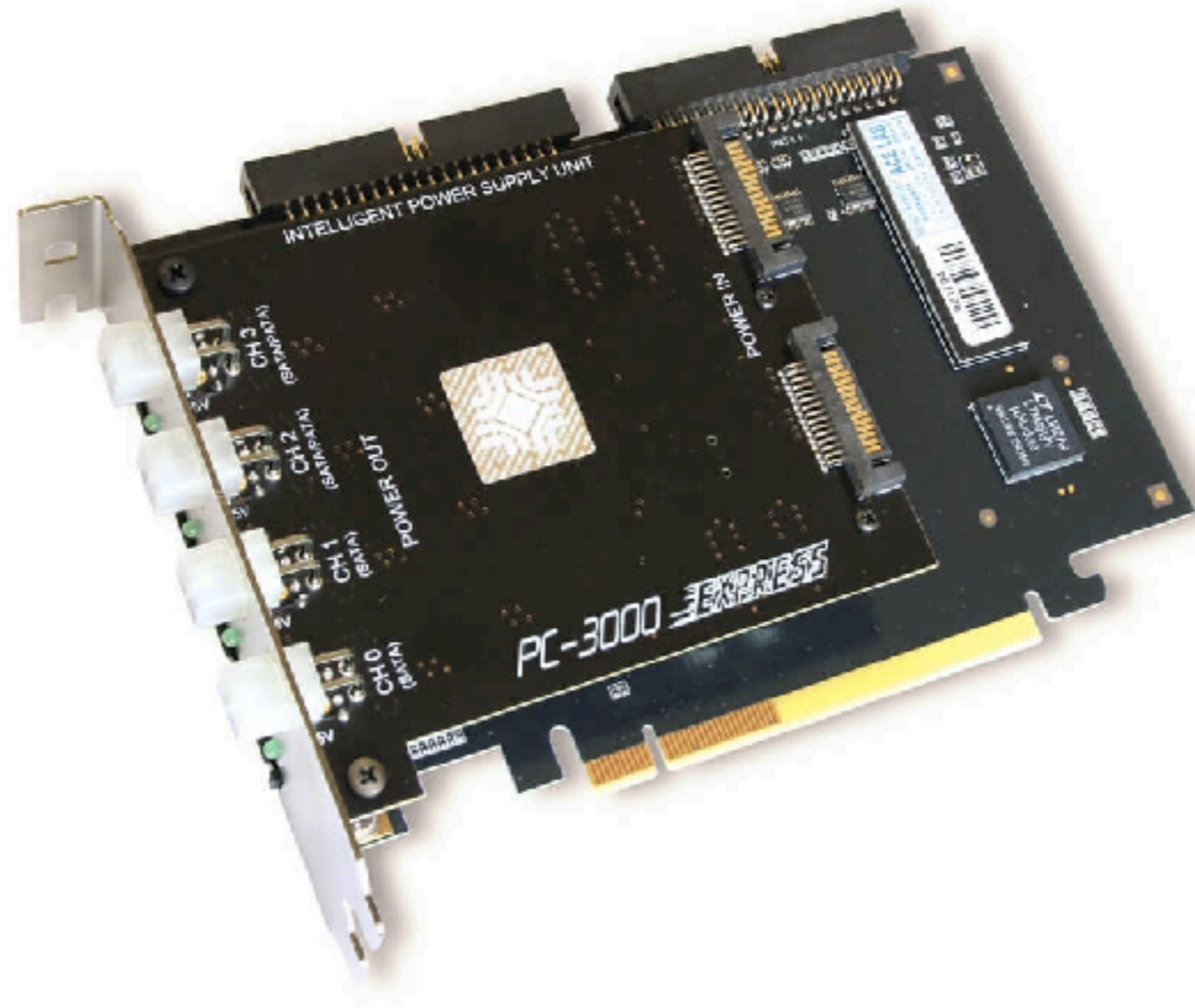
分析出腳位



Seagate UART接線法



發出VSC與串口指令的設備



工廠串口指令

前面工廠手冊有讀寫韌體操作指令
使用Terminal 並且支援Y-Modem協定的軟體

```
F3 T>w30a  
  
File Volume 3  
File ID 30A  
File Copy Number 0  
Start file transfer protocol in 60 seconds.  
CCCCCCCCCCCCCCCC  
File Descriptor FD37430A  
File Size 00001000  
Byte Offset 00000000  
Bytes to write 00001000  
F3 T>_  
  
connected 02:05:01 | Auto detect | 38400 8-N-1 | SCROLL | CAPS |
```


硬碟韌體讀寫指令

指令：

r 為讀取硬碟韌體系統文件

w 為寫入硬碟韌體系統文件

r30a==>讀出模塊30a,

w30a==>寫入模塊30a

```
F3 T>  
ASCII Diag mode
```

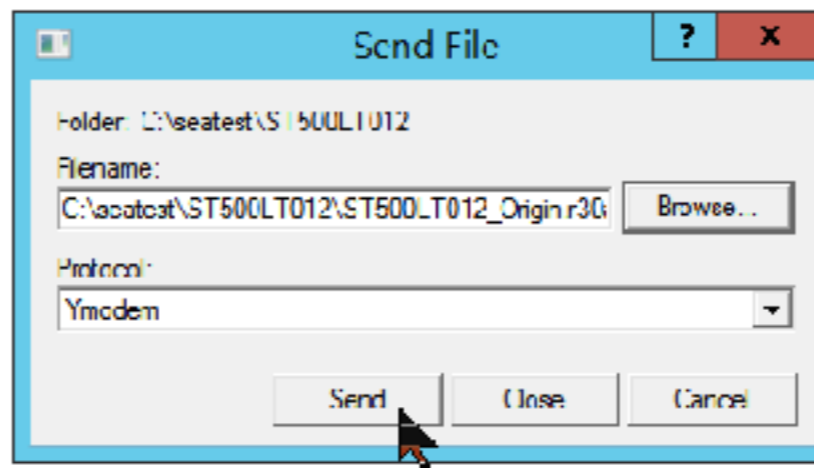
```
F3 T>  
ASCII Diag mode
```

```
F3 I>  
ASCII Diag mode
```

```
F3 T>  
ASCII Diag mode
```

```
F3 T>w30a
```

```
File Volume 0  
File ID 30A  
File Copy Number 0  
Start file transfer protocol in 60 seconds.  
CCCCCCCCCCCCCC_
```



抓取所有硬碟韌體文件

翻遍了技術文件找不到哪邊有密碼相關module
就全部抓取出來

Module	Sys. file	Description
00		Defect list of SA
01	0x001A	Drive information file
02	0x0019	Performance parameter file
03	0x001B	P-List
04	0x003F	SAP (Servo Adaptive FParameters)
05	0x0300	Manufacturin information file
06	0x0001	RAP (Read Adaptives Parameters)
07	0x0208	CAP (Controller Adaptives Parameters)

把所有抓出的韌體區塊做比對

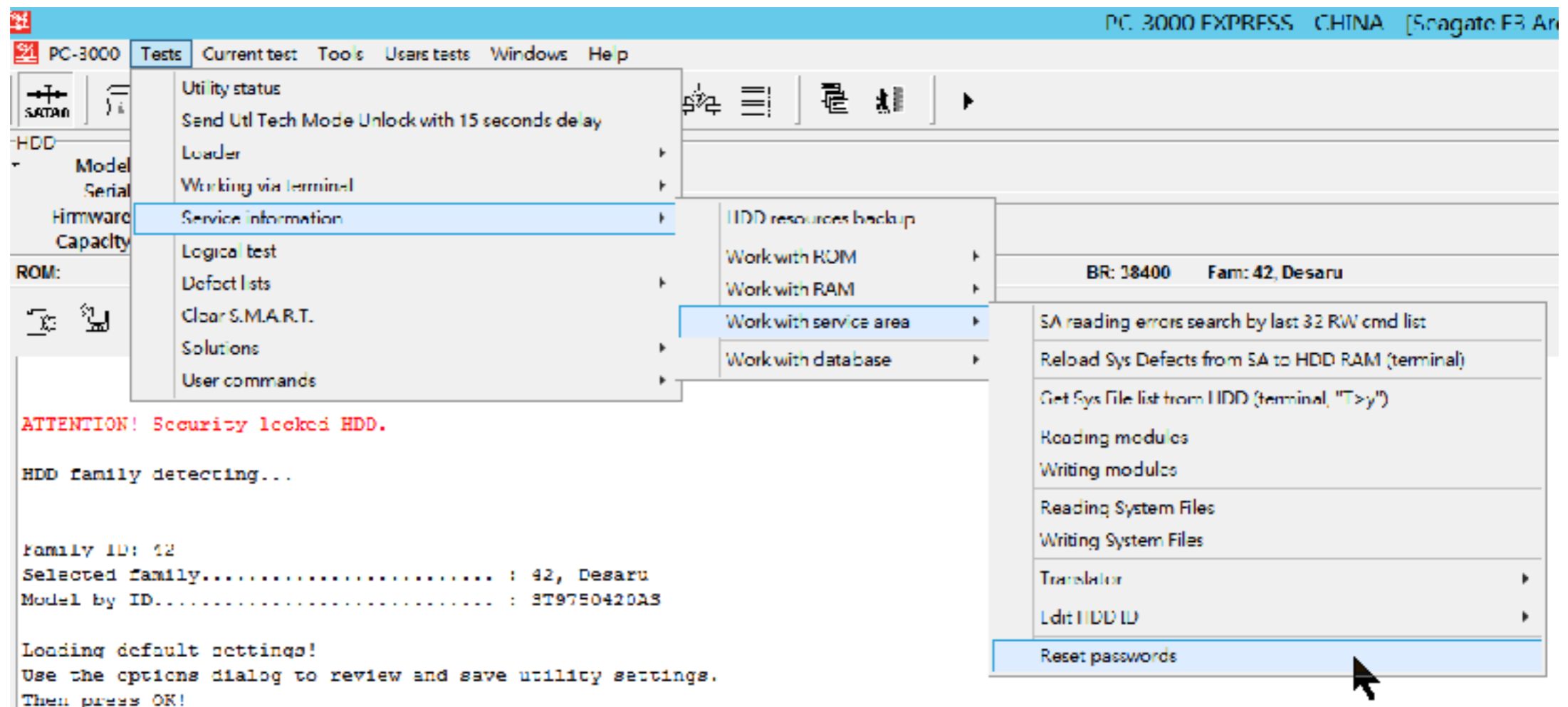
```
SI500L1012_OrigInr30a
Offset  0 1 2 3 4 5 6 7 8 9 A B C D E F  ASCII
00000000  4D 2E 0D 90 FF FF 06 00 11 20 10 10 00 00 FF FF  ip vs | yy
00000010  FF 03 00 00 00 00 00 00 00 00 30 6D 38 3A 00 00  y  '':
00000020  00 00 30 60 38 3A 00 00 00 00 30 6D 38 3A 00 00  '':  '':
00000030  00 00 17 18 2C 60 38 3A 00 00 00 00 00 00 00 00  '':
00000040  00 00 00 00 00 00 00 00 00 00 00 00 12 02 00 00
00000050  02 02 00 00 0C 54 00 00 00 00 23 55 61 57 61 74  1  5e6a
00000060  65 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F  .....
00000070  2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 00 00 00 00 00 00  .....
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000090  00 00 00 00 00 00 00 00 00 00 FF FF 00 00 06 20  .....
00000100  07 06 00 00 00 00 00 00 00 00 1A 6D 07 00 07 00
00000110  7F 00 30 60 38 3A 00 00 00 00 FF 79 15 00 00 00  '':  Yy
00000120  00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000130  00 00 00 00 00 00 00 00 5B 74 29 7D 63 61 59 74  kt.)|u-|
00000140  09 8C 63 61 6F 40 0A 10 00 40 00 00 00 00 00 00  ken g g g R
00000150  FF 37 77 7F 00 00 21 00 77 77 77 77 30 60 30 3A  YYY? 000 0'0:
00000160  00 00 00 00 04 1F 4B 00 50 00 AD 15 AC 09 AC 09  11 8 1-Y-Y
00000170  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
00000180  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
00000190  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001A0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001B0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001C0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001D0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001E0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001F0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
```

發現韌體的30A系統
文件存放ATA密碼
找一樣型號硬碟30A
再用終端回寫回去
即可關閉ATA密碼

```
SI500L1012_NB_PWD_123r30a
Offset  0 1 2 3 4 5 6 7 8 9 A B C D E F  ASCII
00000000  4D 2E 0D 90 FF FF 06 00 11 20 10 10 00 00 FF FF  ip vs | yy
00000010  FF 03 00 00 00 00 00 00 00 00 30 6D 38 3A 00 00  y  '':
00000020  00 00 30 60 38 3A 00 00 00 00 30 6D 38 3A 00 00  '':  '':
00000030  00 00 17 18 2C 60 38 3A 00 00 00 00 00 00 00 00  '':
00000040  00 00 00 00 00 00 00 00 00 00 00 00 12 02 00 00
00000050  02 02 00 00 0C 54 01 01 00 00 72 55 61 50 60 29  1  1U-6'0
00000060  00 2F 2F 57 6C 7D 7D 9F 00 2F 7D 03 23 77 01 00  .....
00000070  71 D3 DA F1 CC E0 C9 D0 30 7F 72 55 61 70 60 A8  qd'iiE' pprUe0' :
00000080  00 2B D6 52 60 1D 1D 9E 09 AF 0D 03 23 77 91 00  +F'iiE' m tv'
00000090  71 D3 DA F1 CC E0 C9 D0 30 7F 01 40 04 00 06 20  qd'iiE'F' 00 0
00000100  07 06 00 00 00 00 00 00 00 00 1A 6D 07 00 07 00
00000110  7F 00 30 60 30 3A 00 00 00 00 FF 79 15 00 00 00  '':  Yy
00000120  00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000130  00 00 00 00 00 00 00 00 6B 74 29 7D 63 61 6B 74  kt.)|u-|
00000140  09 8C 63 61 6F 40 0A 10 00 40 00 00 00 00 00 00  ken g g g R
00000150  FF 37 77 7F 00 00 27 01 77 77 77 77 30 60 30 3A  YYY? 000 0'0:
00000160  00 00 00 00 04 1F 4B 00 50 00 AD 15 AC 09 AC 09  11 8 1-Y-Y
00000170  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
00000180  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
00000190  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001A0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001B0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001C0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001D0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001E0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
000001F0  AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59 AC 59  -Y-Y-Y-Y-Y-Y-Y-Y
```



看看專業怎做的



分析專業設備的方法

The image displays two screenshots of a hex editor. The top screenshot shows a memory dump with the following data at offset 0x56:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000560	01	01	00	00	00	00	00	00	00	72	55	61	70	60	20	

The bottom screenshot shows the same memory dump after modification, with the data at offset 0x56 changed to:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000560	00	00	00	00	00	00	00	00	00	72	55	61	70	60	20	

發現PC3000 並不是使用修改 ATA密碼並沒有改變 但是有類似ATA密碼開關,位置在30a韌體系統文件 offset 0x56和0x57 只要改為0000 再用終端回寫回去即可關閉ATA密碼

Live demo 用串口破解IBM 筆記型電腦 硬碟加密

其他方法

1.熱交換

2.ROM中的韌體缺陷表

都是利用打斷正常啟動流程

如何獲得硬體用的工廠指令集

泄露的工廠技術文件

測錄會發出工廠指令軟體

逆向工程

窮舉Fuzzer指令集

泄露的工廠技術文件

比如剛剛前面希捷的文檔
就有詳細終端指令與ATA 工廠指令。

天下文章一大抄

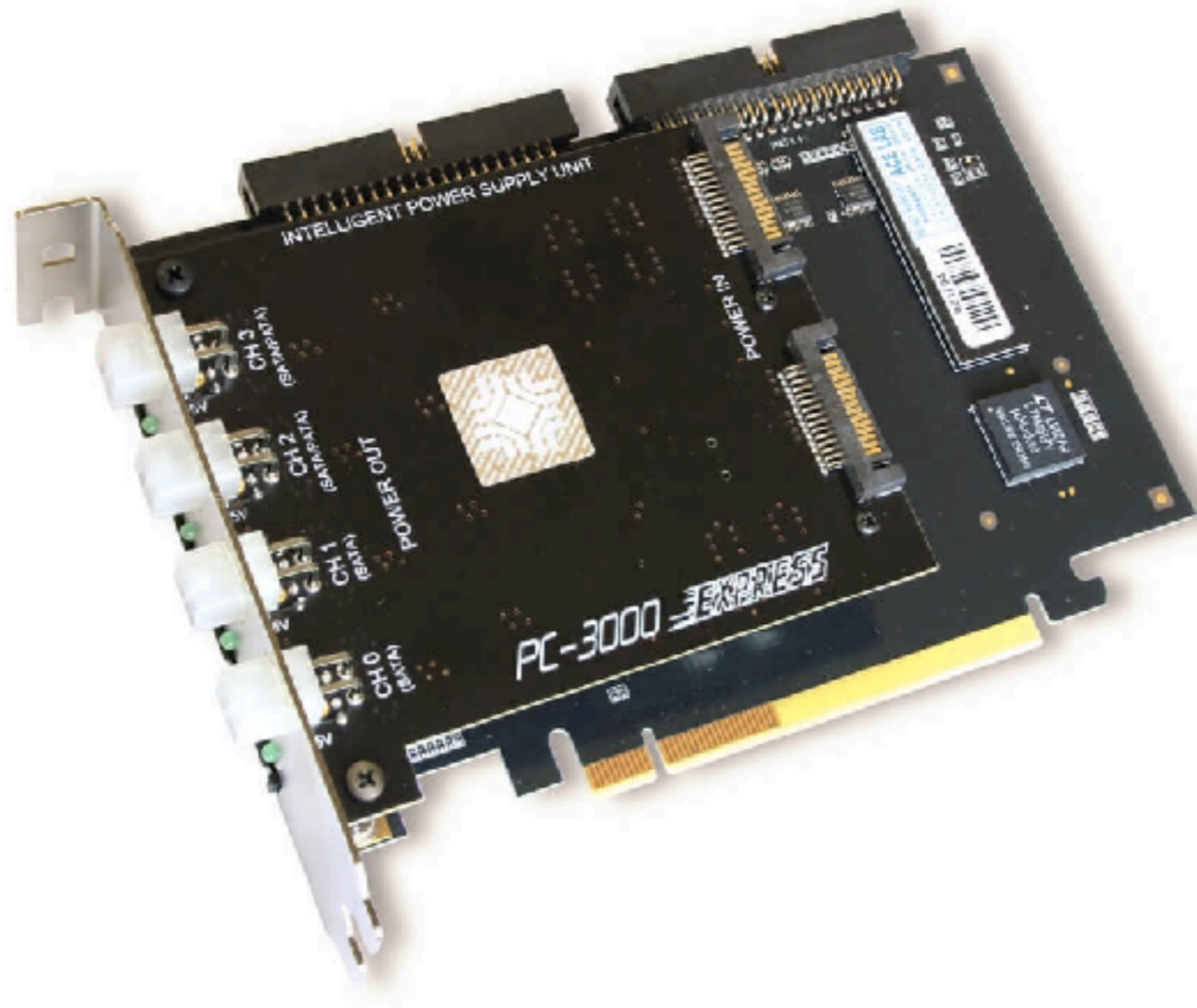
Sniffer會發出VSC 的軟硬體

一.工廠內部軟體

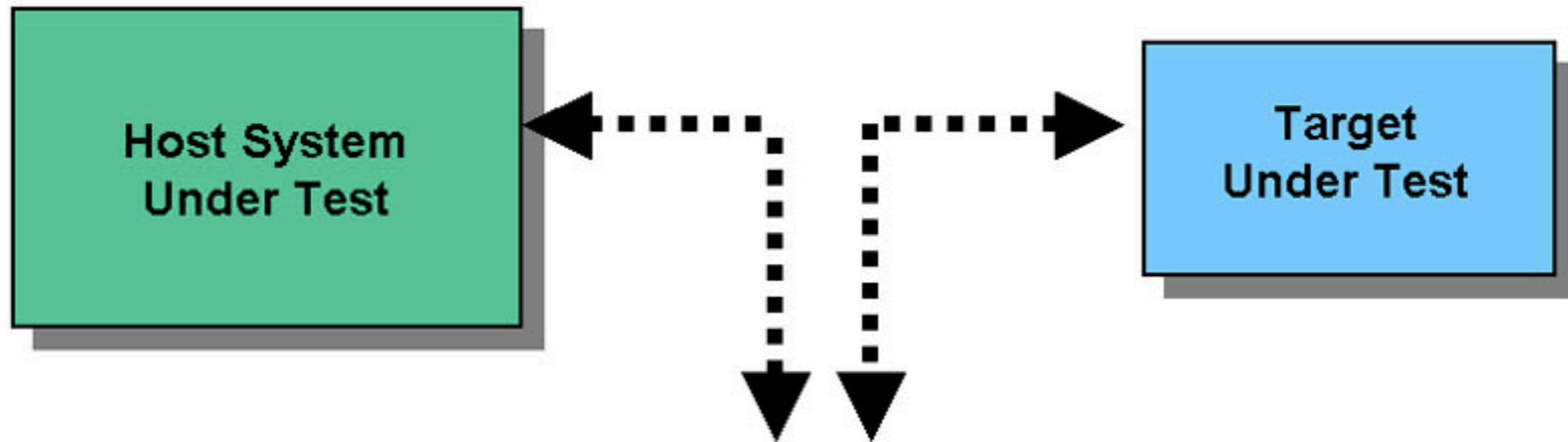
二.韌體升級軟體

三.非官方資料救援設備硬體與軟體

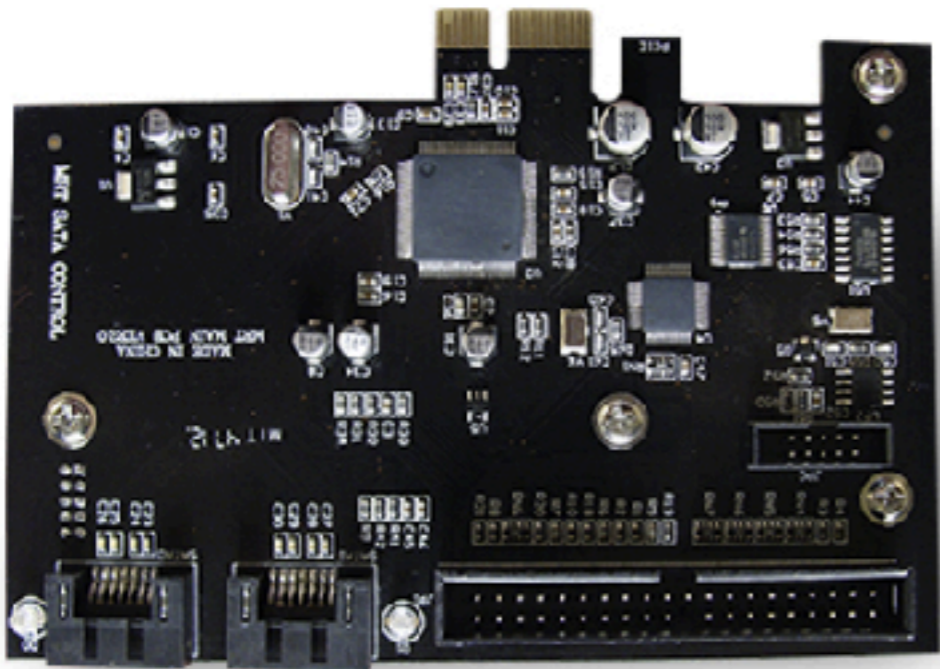
發出VSC的非原廠硬體



SATA 邏輯分析儀



資安硬體界的黑吃黑



逆向工程靜態分析

直接分析rom bin,通過IDA反組譯韌體

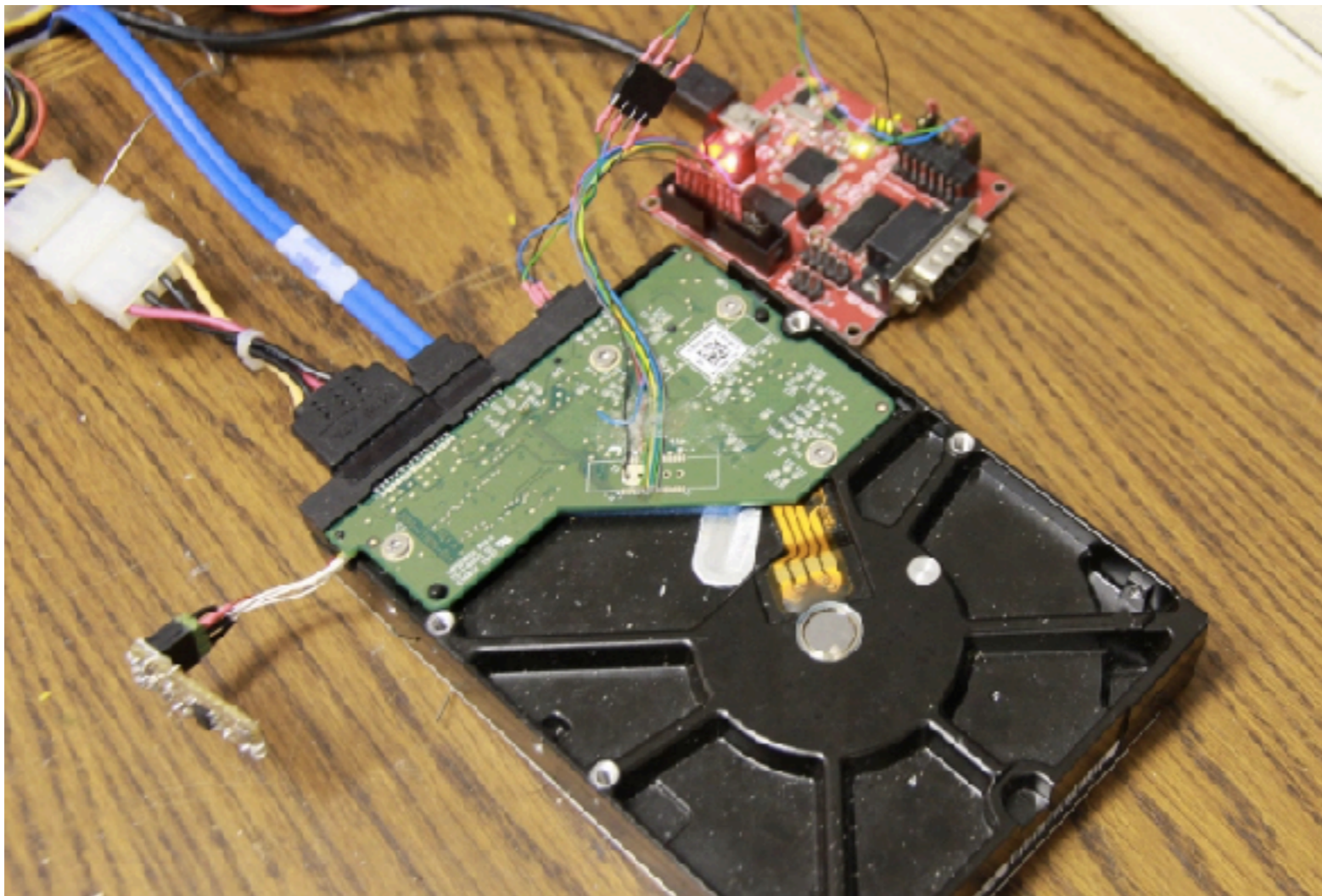
embedded系統大部分是基於ARM或者MIPS內核的CPU的
可用IDA來反組譯

韌體裡面通常有一個命令解析引擎

反組譯命令解析引擎的代碼，就可以知道設備支持哪些指令
包括vender commands，並且能推導出commands詳細的參數

使用JTAG動態反組譯

有動態反彙編的，就是通過連接JTAG調試接口，這樣可以動態運行，並動態下中斷點



窮舉Fuzzer指令集

窮舉可能的命令代碼，ATA命令code裡面有專門的reserved號段和Vendor Spec號段，這些就是專門為vender commands保留的

通常vender commands就會使用這些保留命令碼段

會寫成測試小工具，然後再硬盤上面跑

如果監測到硬碟有反應，就記錄下來，最後人工來篩選這些結果，看看有沒有用得上的東西

嵌入式系統 攻與防反制

硬體Hash反制

關掉硬體Port

硬碟韌體防火牆

NSA 美國國安局的陰謀

硬體Hash反制

```
&>  
(1Ah) - 解鎖前, Serial Port被關閉  
&>  
(1Ah) - TCG Serial Port Disabled  
&>  
(1Ah) - TCG Serial Port Disabled  
&>  
(1Ah) - TCG Serial Port Disabled
```

Tech Unlock Handshake: 0x1CEF53D8

Reply:

Tech Unlock Handshake: 0x5194FCFE

Reply:

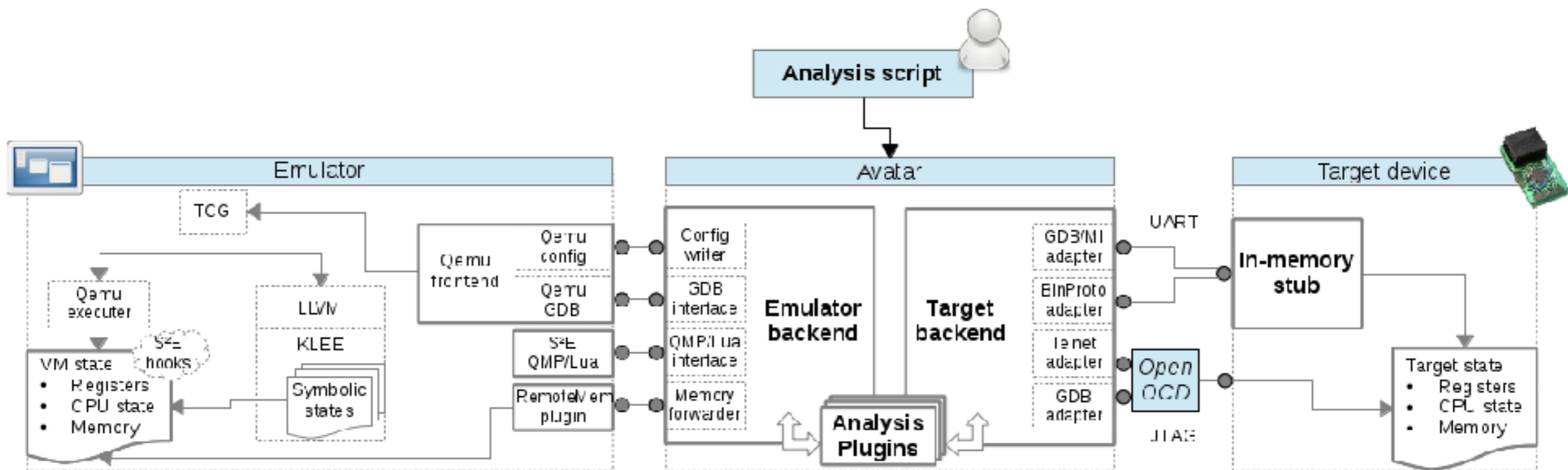
Spin Up

SpinOK

(P) SATA Reset

ASCII Diag mode

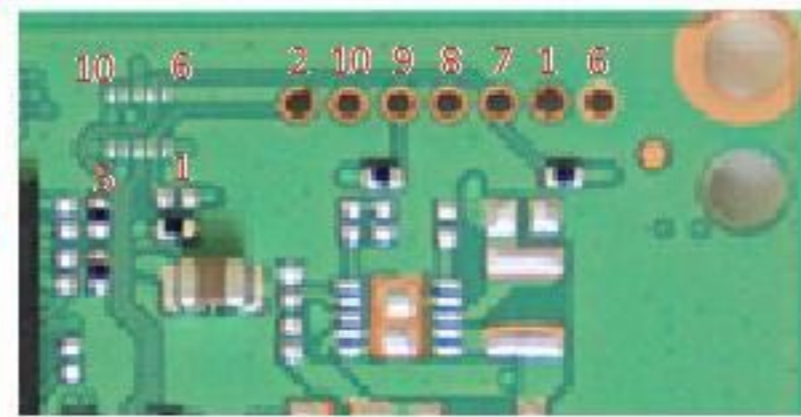
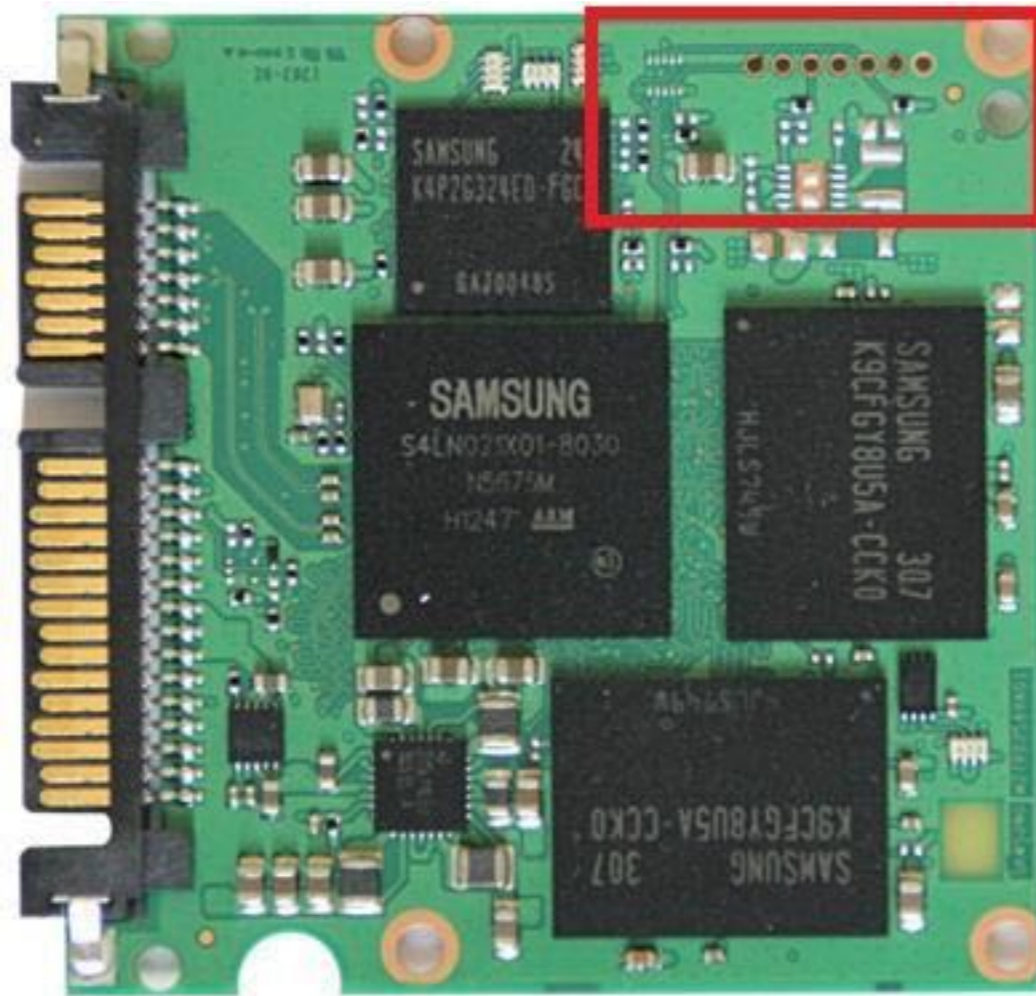
每次解鎖後所得代碼都不同，
所以不是固定代碼，而是某種
演算所產生的代碼



結束

應用與原理必須相結合

Q&A



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000000000000	25	B0	EE	8A	EE	EF	A6	22	18	2B	8D	32	15	98	E2	E2	%*i i "+ 2 ââ
000000000010	C3	B3	6D	C5	BD	FF	20	FA	E9	43	7E	AE	0E	69	0C	ED	Ã³mÃ¼ý úéC~@ i i
000000000020	CB	84	FB	90	7F	D4	F8	91	AE	CA	37	B9	33	8F	47	61	Ë ú Ôø'@Ê7'3 Ga
000000000030	E3	12	82	58	4B	CD	34	6E	12	12	F8	47	D9	5F	29	49	ã XKÍ4n øGÛ_)I
000000000040	8F	26	2C	E3	8B	5D	88	FC	7D	E4	92	18	C3	59	CD	2F	&.ã } ü}ä' ÅYÍ/
000000000050	44	32	9A	A6	DF	98	D7	ED	A2	27	39	D7	6E	1D	C7	D5	D2 B ×ic'9xn çÕ
000000000060	6D	90	27	67	7C	F2	F0	84	23	54	C2	13	82	01	BA	15	m 'g òð #TÅ °
000000000070	51	34	C1	72	54	5B	55	B8	82	C4	A7	64	1A	35	F8	5E	Q4ÁrT[U, Å\$ d 5ø^
000000000080	81	7F	4E	4A	9E	F1	FB	70	A3	1D	17	58	1C	3D	7B	3C	NJ ñúpf X ={<
000000000090	50	7B	5E	71	37	94	D3	A6	D7	1C	1C	4D	8A	9D	FB	BE	P{^q7 Ó × M ú% + 8 . i U0 8
0000000000A0	2B	8E	16	7F	15	38	14	2E	0E	ED	0C	55	30	9C	99	38	8#IHj] S÷;%.%bö
0000000000B0	38	23	CD	48	6A	5D	9D	53	F7	3B	25	2B	2E	25	62	F6	áäv =YÉd8 ÅK 4¶
0000000000C0	E1	E4	76	07	3D	59	CB	64	38	94	C4	4B	9D	8A	34	B6	kpÛiý p F øÅÕéiN
0000000000D0	6B	FE	D9	EC	FF	20	70	10	46	14	F8	C2	D5	EA	EC	4E	VqCf iz s` / Ë
0000000000E0	56	71	43	66	88	EE	7A	12	73	A8	82	8B	2F	9B	CB	20	É@>Ö`Z [Á áóK,
0000000000F0	C9	A9	3E	D6	A8	5A	93	5B	20	C1	7C	14	E2	F3	4B	B8	ÅXÆi éÔ@³.\`Å^°
000000000100	C2	58	C6	EE	99	10	EA	D2	A9	B3	2E	5C	27	C5	5E	B0	Đó 'ÕË@Ûö.± I
000000000110	D0	F3	1E	14	93	27	D5	CB	AE	D9	F6	2E	B1	0B	8B	49	dl:C û K ¶*Z
000000000120	64	6C	3A	43	9B	FB	03	05	14	A6	4B	7F	B6	B0	5A	09	■tYi·i @Wúú ô i
000000000130	1F	74	59	EF	B7	EE	7C	19	AE	57	FA	FB	04	F4	21	EF	(#%. i{c6µa <N
000000000140	28	9E	23	BE	2E	88	EE	7B	63	36	B5	61	1E	3C	4E	13	upYstöD ÈÛ N"Å÷e
000000000150	75	B5	59	73	74	F6	44	00	C8	DC	99	4E	22	C5	F7	65	z-Ì± ö±5W à- Û
000000000160	7A	AD	CC	B1	94	12	06	F6	B1	35	57	20	E0	AD	00	D9	KI B(Å ð'?'áF> B
000000000170	4B	49	03	42	28	C2	94	F0	B2	3F	BA	E1	46	3E	86	DF	ò@É é ÅâeI H
000000000180	F2	A9	C9	0F	03	E9	0D	7C	01	C2	E2	65	49	1A	17	48	Õ xuidæK ýløm`
000000000190	D5	80	9A	D7	75	EF	64	E6	4B	15	02	FD	31	F8	6D	60	` % 0I Î . iV
0000000001A0	92	94	BD	8B	30	49	94	CE	0A	2E	8B	81	06	1F	EE	56	<lBI`d6Älú%p ËÛ
0000000001B0	AB	6C	42	49	A8	64	36	C4	31	FC	BC	70	97	C9	D9	82	'` wOæ'È-X i~ø
0000000001C0	27	91	8E	89	77	4F	E6	27	C8	AC	58	05	EC	7E	7E	F0	n7 ÷ Lsfñ-J@´
0000000001D0	06	6E	37	93	F7	9D	7C	1C	09	4C	73	F1	AD	4A	A9	B4	Ë 0u% >³; pw
0000000001E0	94	95	CB	A0	0D	30	75	BE	94	18	3E	AA	3B	8C	70	77	3U \$ >øÖKýÅ ,
0000000001F0	8D	1F	33	55	83	9D	24	9C	3E	F8	D6	4B	FF	41	89	B8	

WD 硬碟重要參數

The screenshot shows the MRT application interface with the following sections:

- 硬盘信息 (Disk Information):**
 - 型号: WDC WD5000AAKS-22A7D0
 - 序列号: WD-WMASY1114341
 - 固件版本: 01.03B01
 - 容量: 976773168 (465.76 GB)
- 其它信息 (Other Information):** (highlighted with a red box)
 - 家族: Atlantis
 - SA Cyl: 170 Head: 4 SPT: 1311
 - ROM版本: 02.38C
 - 启动模式: 普通模式
- 最近操作 (Recent Operations):** N/A
- 任务信息 (Task Information):** N/A

The main text area displays the following diagnostic output:

```
Technology node 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 : ..... : 02.38C
ROM generation : ..... : 02.38C
Link table version : ..... : 03.8H
ROM Firmware version : ..... : 0002003R

ROM Modules:
```

The value **0002003R** is highlighted with a red box.

At the bottom, the **Power** status is **ON**, and the **Status (ATA1)** section shows **DSY** and **DSD** as active indicators.

ROM微代碼版本號

The screenshot shows a diagnostic application window with the following sections:

- 硬盘信息 (Hard Disk Info):**
 - 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 (Other Info):**
 - 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 (Recent Operations):** 诊断 -> 服务区操作 -> ROM操作 -> ROM列表
- 任务信息 (Task Info):** N/A
- ROM列表 (ROM List):** 4F.bin
- Hex Dump Table:**

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....0...._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	FBU.....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	00a...F.
000000A0	05	00	18	00	92	08	C0	E3	75	FF	91	FB	18	00	0C	00u.....
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

At the bottom, there is a status bar with the following indicators:

- Power: ON
- Status (ATA1): BSY, DRD, DNF, DSC, DRQ, CRR, IDX, ERR
- Error: BBK, UNC, INF, ABR, TON, AMN

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 **重要模塊一丟失 資料一去不復返**

韌體防火牆Firewall

- 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
阻斷 軟體對硬碟發出 VSC指令