解析
儲存embedded架構原理實現漏洞與反制

OSSLab

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？

OSSLab

講師介紹

Thx(熊大)

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

OSSLab

儲存裝置上的嵌入式架構

CPU Core + RAM

ROM

碟片上的韌體架構

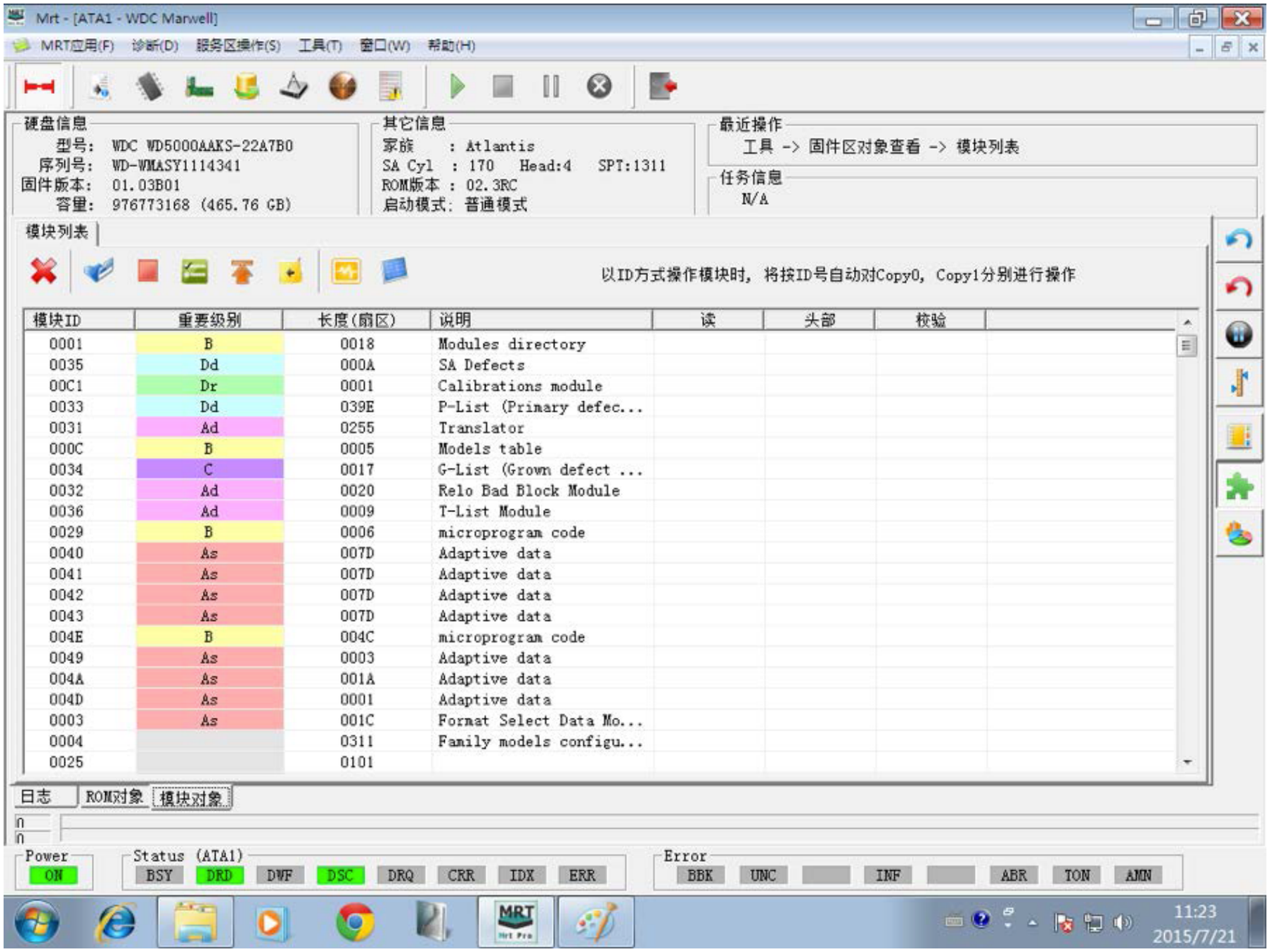
OSSLab

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 embedded system
  不同的是儲存韌體地方會二個位置
  ROM+碟片

OSSLab

WD 碟片上韌體模塊列表



OSSLab

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 (請慎防不肖資料業者亂改)

OSSLab

中斷硬碟啟動流程

硬碟安全系統有啟用時,硬碟開機就會進入韌體安全系統,鎖住硬碟資料.

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.

這二種狀況是一樣的 可以用打斷正常啟動流程

破解儲存安全保護

資料救援恢復嚴重損壞韌體硬碟

OSSLab

ATA Vendor-specific command (工廠指令集)

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

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 various implementations.

OSSLab

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							

OSSLab

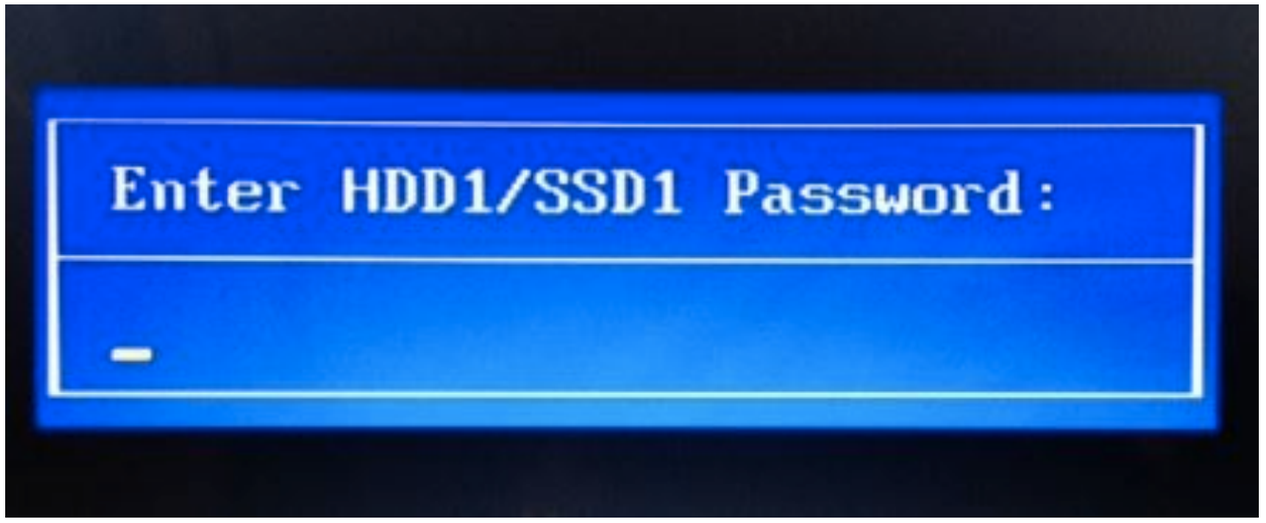
儲存裝置安全保護

ATA 保護

AES 加密

韌體 保護

ATA 加密

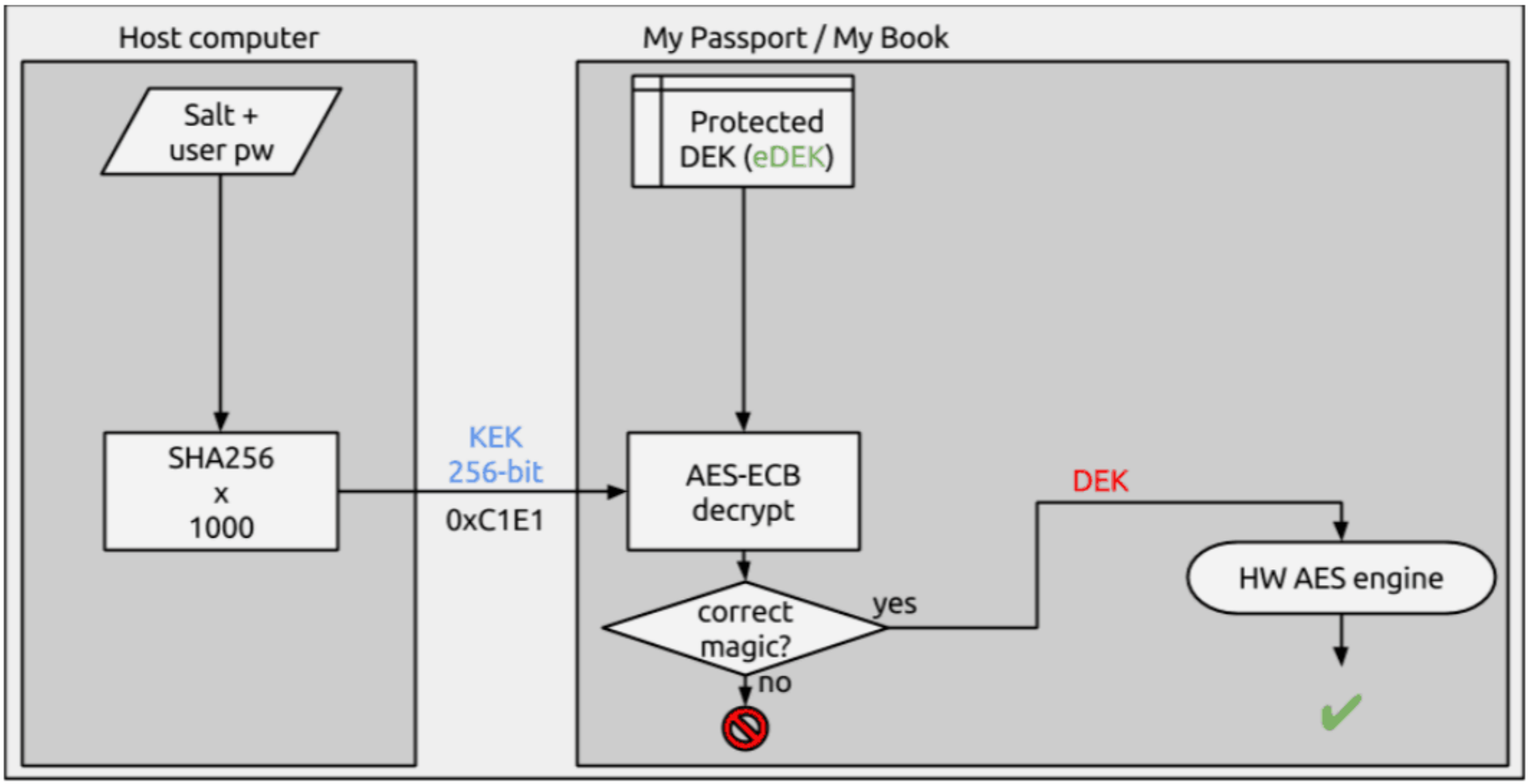


OSSLab

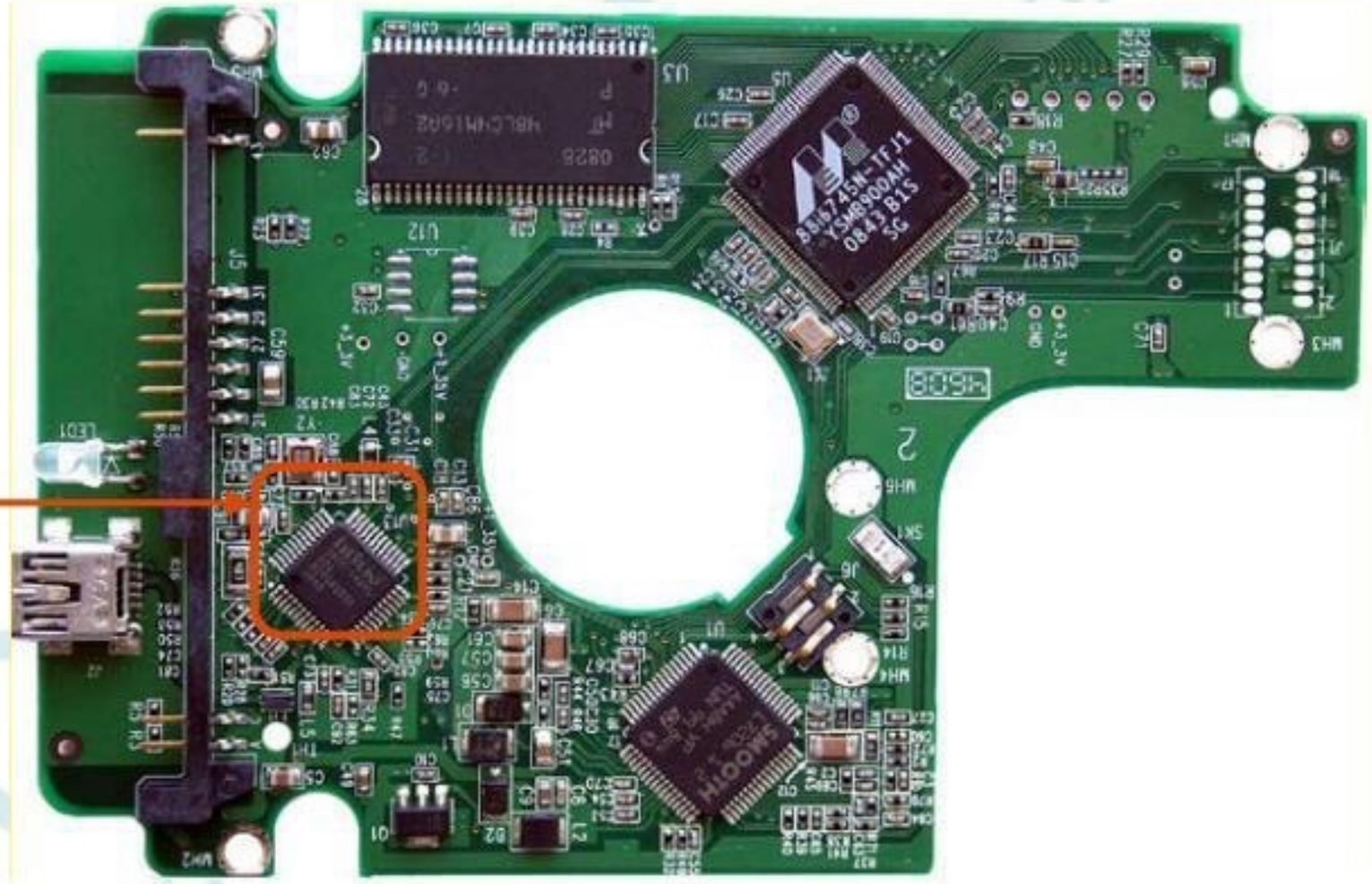
AES 加密硬碟

OSSLab

AES 加密

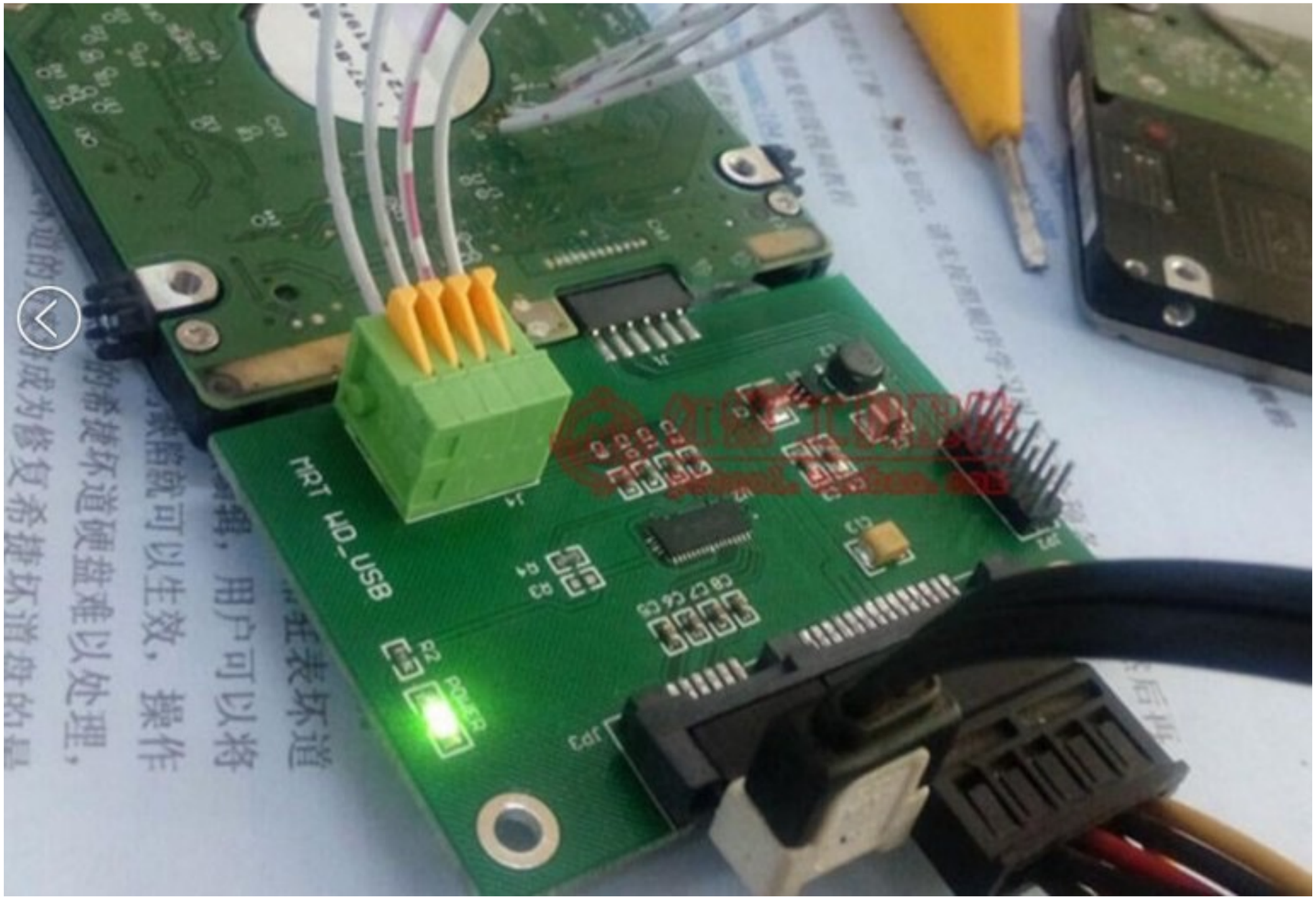


OSSLab



OSSLab

OSSLab



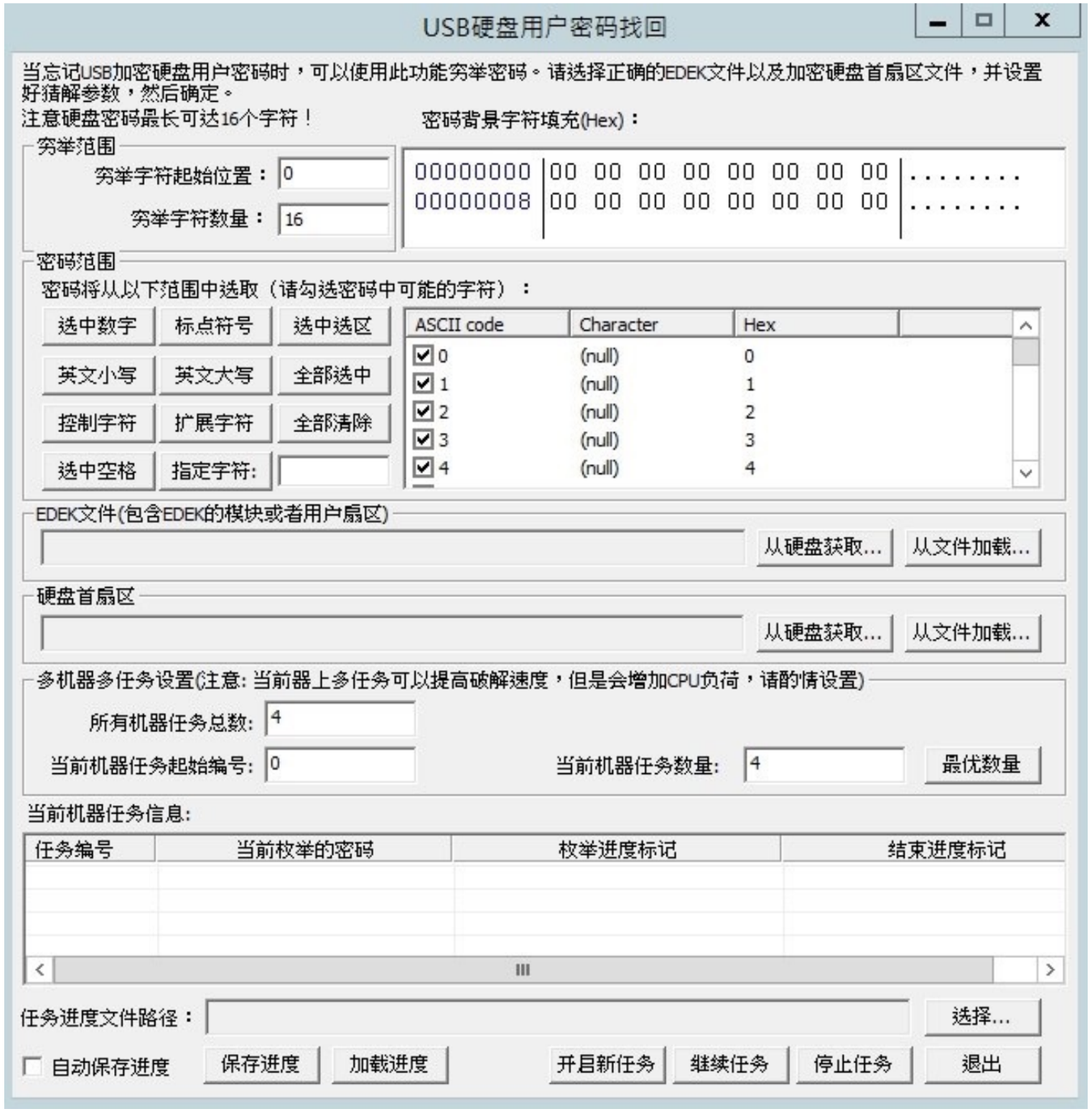
OSSLab

mbr.bin

```
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  ü1ÀŽÐ1äŽØŽÀ¾.|¿.
00000010   06 B9 00 01 F3 A5 BE EE 07 B0 08 EA 20 06 00 00  .¹..ó¥¾î.°.ê ...
00000020   80 3E B3 07 FF 75 04 88 16 B3 07 80 3C 00 74 04  €>³.ÿu.ˆ.³.€<.t.
00000030   08 06 AF 07 83 EE 10 D0 E8 73 F0 90 90 90 90 90  ..¯.fî.Ðèsð.....
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  ..............¾¾
00000080   07 B0 00 B9 04 00 80 3C 00 75 6E FE C0 83 C6 10  .°.¹..€<.unþÀƒÆ.
00000090   E2 F4 31 DB B4 0E BE 9D 07 8A 0E AF 07 AC D0 E9  âô1Û´.¾..Š.¯.¬Ðé
000000A0   73 02 CD 10 08 C9 75 F5 B0 3A CD 10 31 C0 CD 16  s.Í..Éuõ°:Í.1ÀÍ.
000000B0   3C 00 74 F8 BE 8B 07 B9 02 00 E8 BA 00 3C 0D 74  <.tø¾‹.¹..è°.<.t
000000C0   B4 3C 61 72 06 3C 7A 77 02 2C 20 88 C3 BE 9D 07  ´<ar.<zw., ˆÃ¾..
000000D0   8A 0E AF 07 AC D0 E9 73 04 38 C3 74 06 08 C9 75  Š.¯.¬Ðés.8Ãt..Éu
000000E0   F3 EB AF B8 0D 0E 31 DB CD 10 8D 84 62 00 3C 07  óë¯¸..1ÛÍ..„b.<.
000000F0   75 07 B0 1F A2 AF 07 EB 99 31 D2 B9 01 00 3C 04  u.°.¢¯.ë™1Ò¹..<.
00000100   74 11 73 F3 30 E4 B1 04 D2 E0 BE BE 07 01 C6 8A  t.só0ä±.Òà¾¾..ÆŠ
00000110   16 B3 07 BF 05 00 56 F6 C2 80 74 31 B4 41 BB AA  .³.¿..VöÂ€t1´A»ª
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.‹\.¾..‰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 B6 EA 00 7C 00  u´ë“.>þ}Uªuöê.|.
00000170   00 BE 83 07 B9 0A 00 50 B4 0E 31 DB AC CD 10 E2  .¾ƒ.¹..P´.1Û¬Í.â
00000180   FB 58 C3 54 65 73 74 44 69 73 6B 0D 0A 10 00 01  ûXÃTestDisk.....
00000190   00 00 7C 00 00 00 00 00 00 00 00 00 00 00 31 32 33  ..|..........123
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  ...þÿ™?...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 55 AA  ..............Uª
```

Partition table

OSSLab



WD AES 暴力破解

OSSLab

我在路上撿到工廠指令手冊

OSSLab

請你跟我這樣做(一)

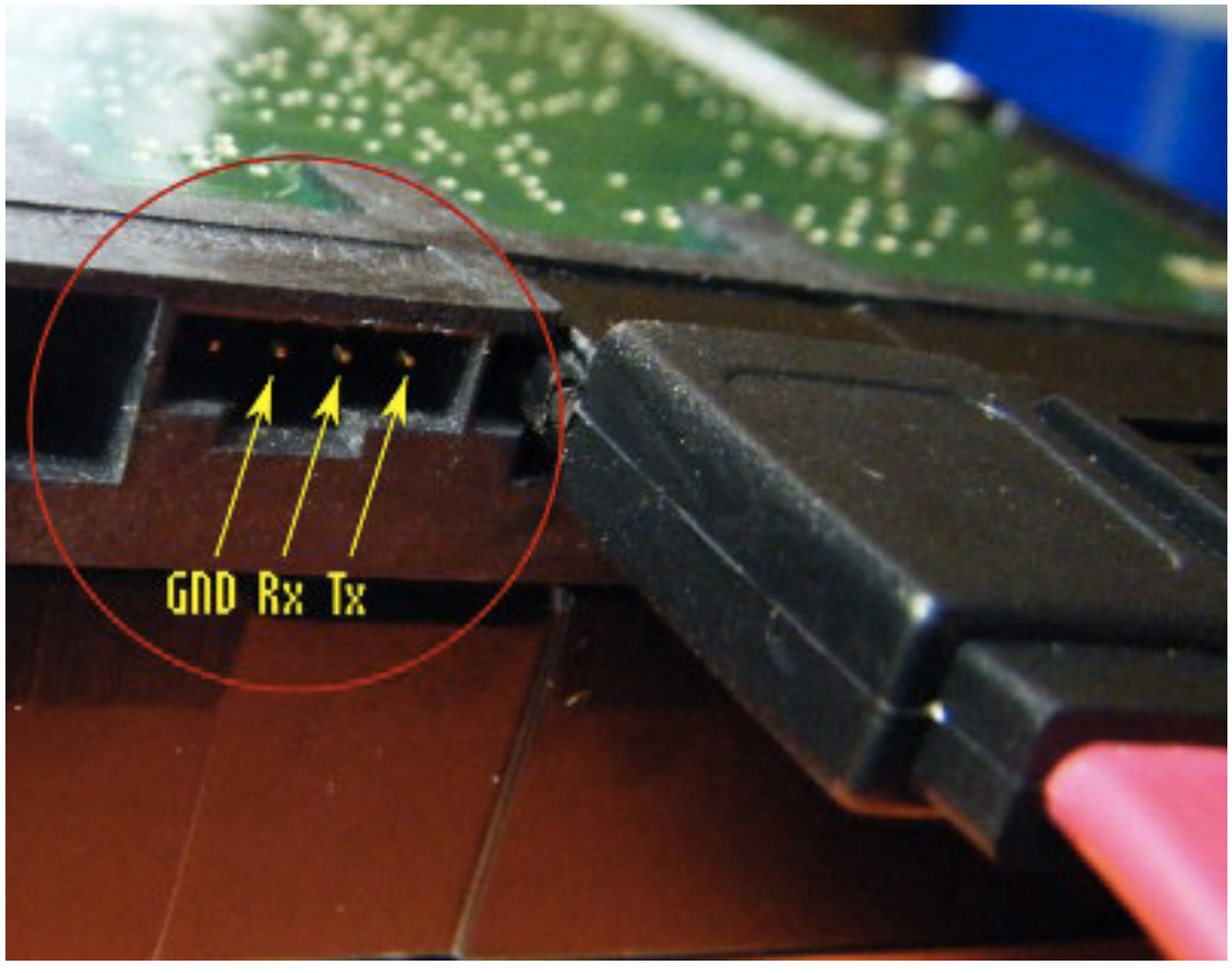
Seagate
F3 Serial Port Diagnostics

F3 串行端口诊断命令
中文翻译

（Rev.TR30）

OSSLab

請你跟我這樣做(二)



OSSLab

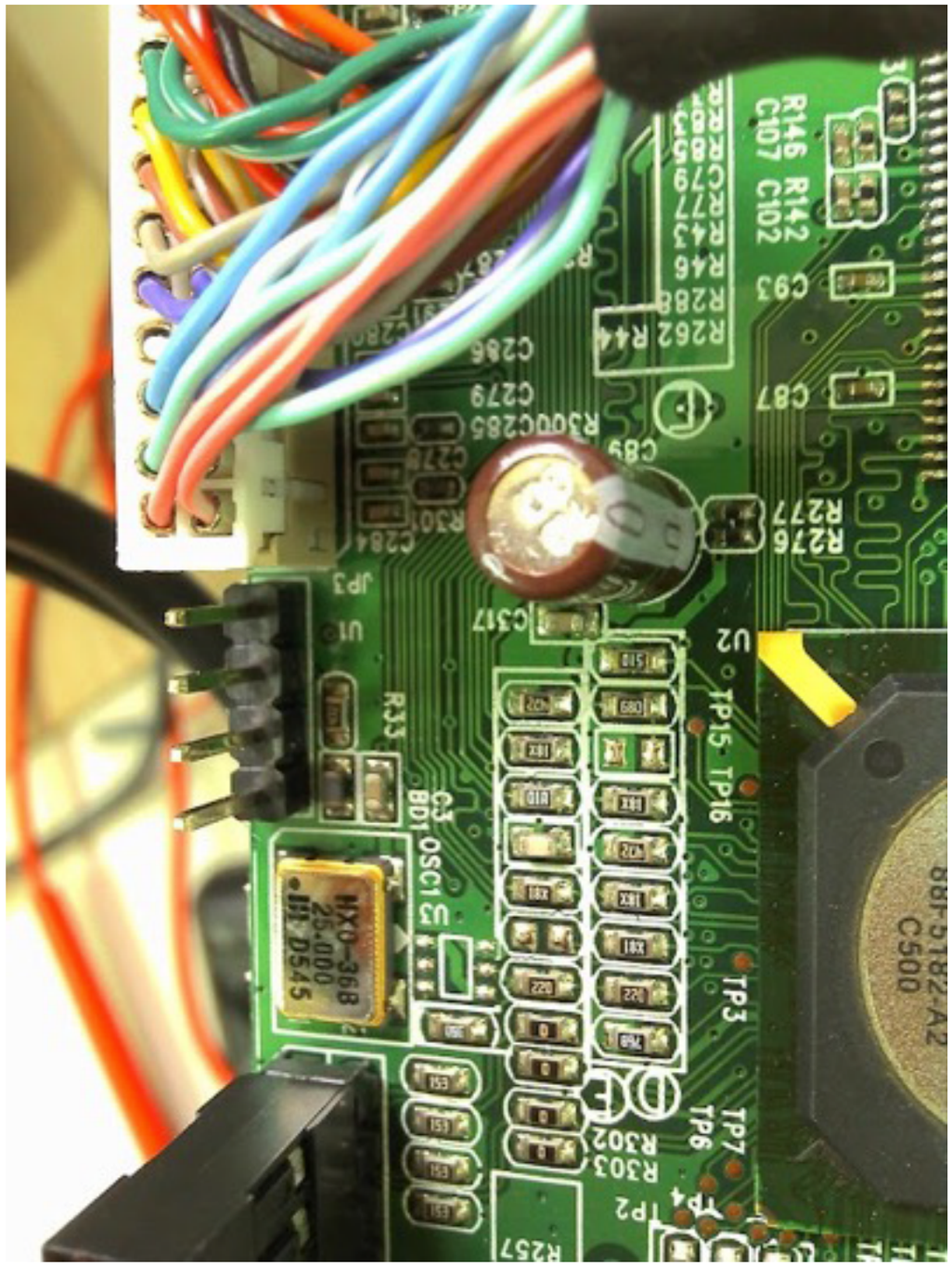
Serial TTL (UART)通訊

- 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)

OSSLab

逆向Serial UART腳位



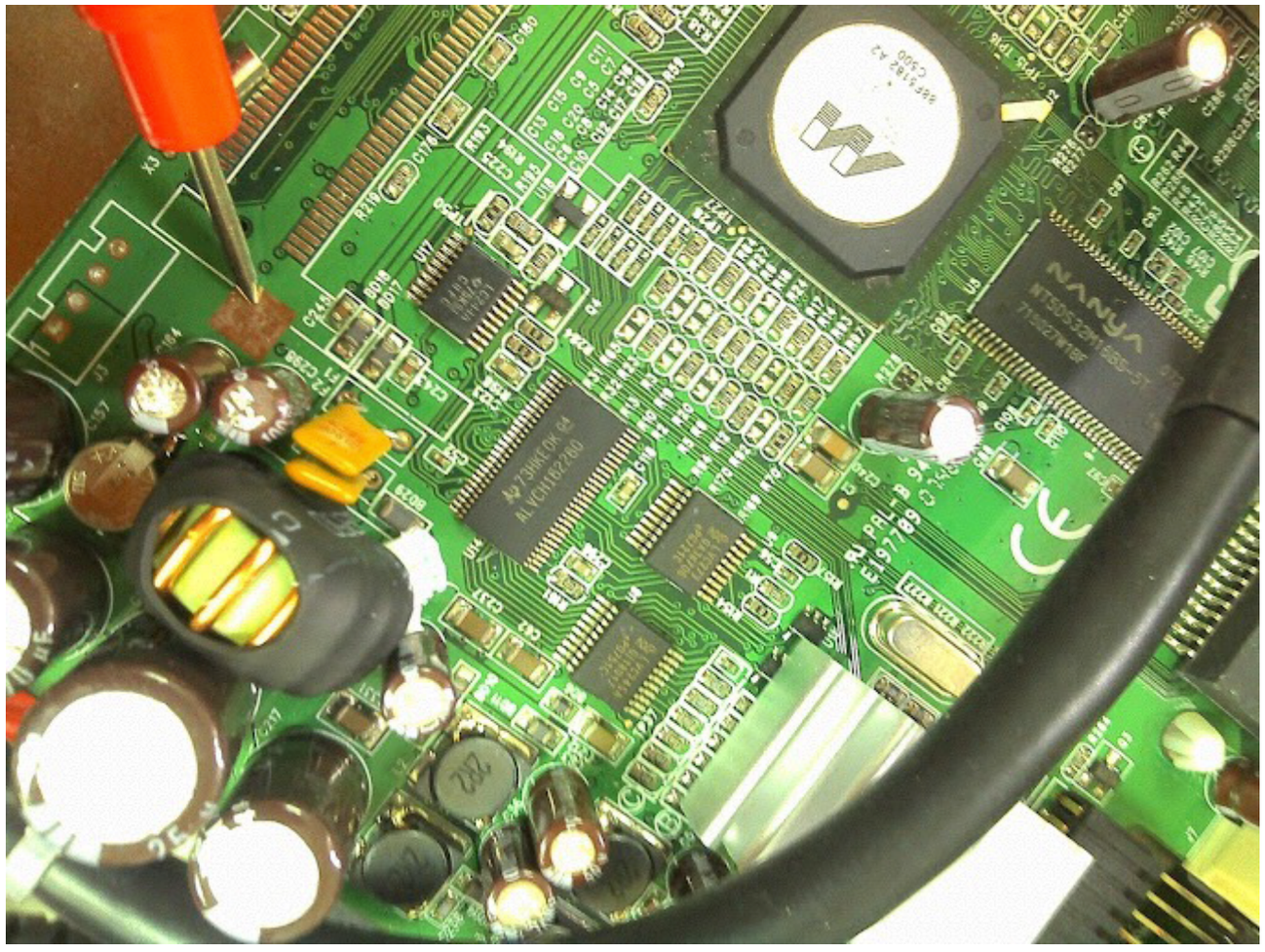
- 以一台ARM NAS做範例

OSSLab

GND腳位判定

- 最好抓的是GND

- 先將embeeded 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)



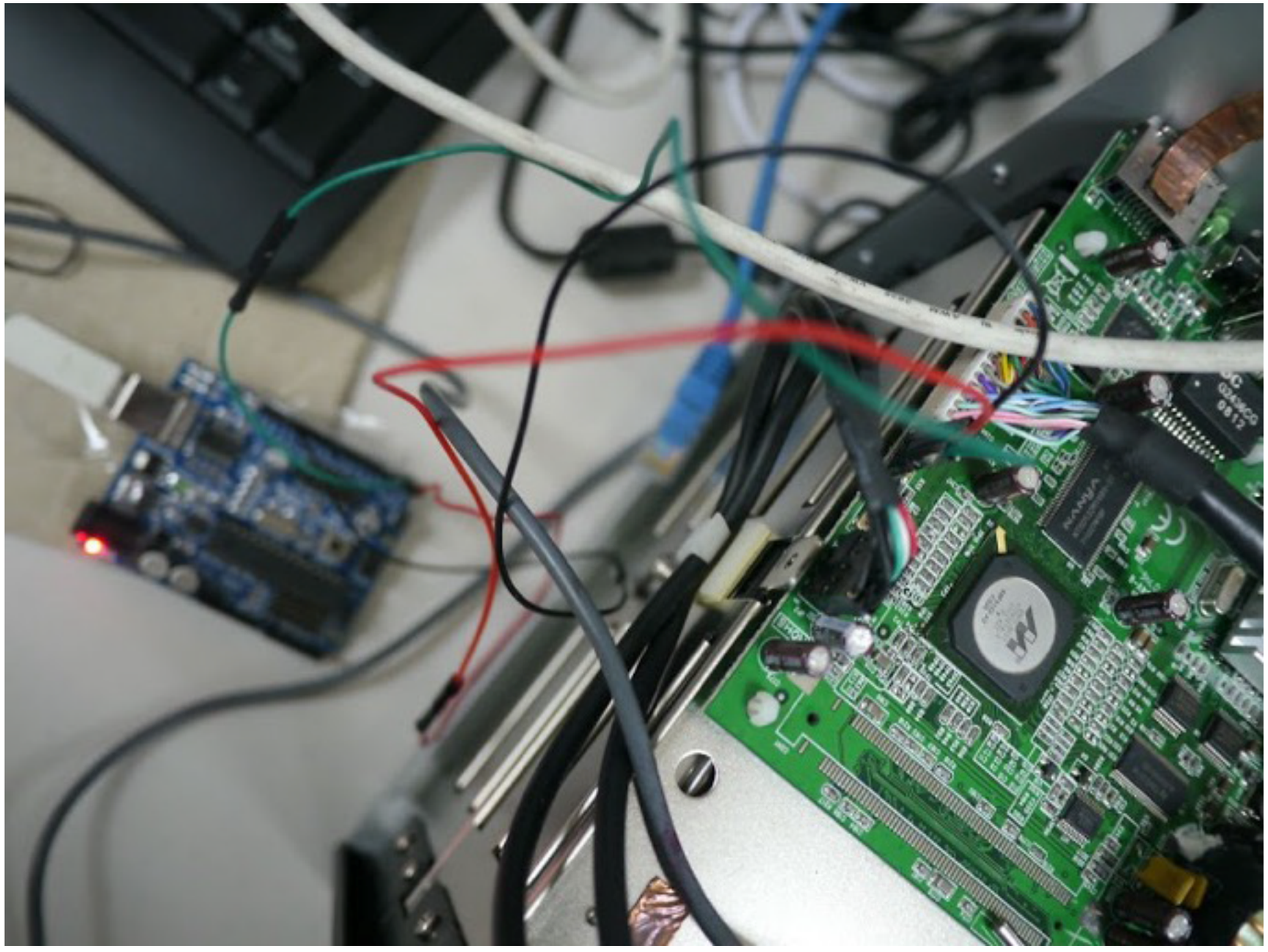
- 另外一邊探針 則每個Pin都試, 發現第一根有跟接地點導通, 會翁鳴。
  因此第一根為GND

OSSLab

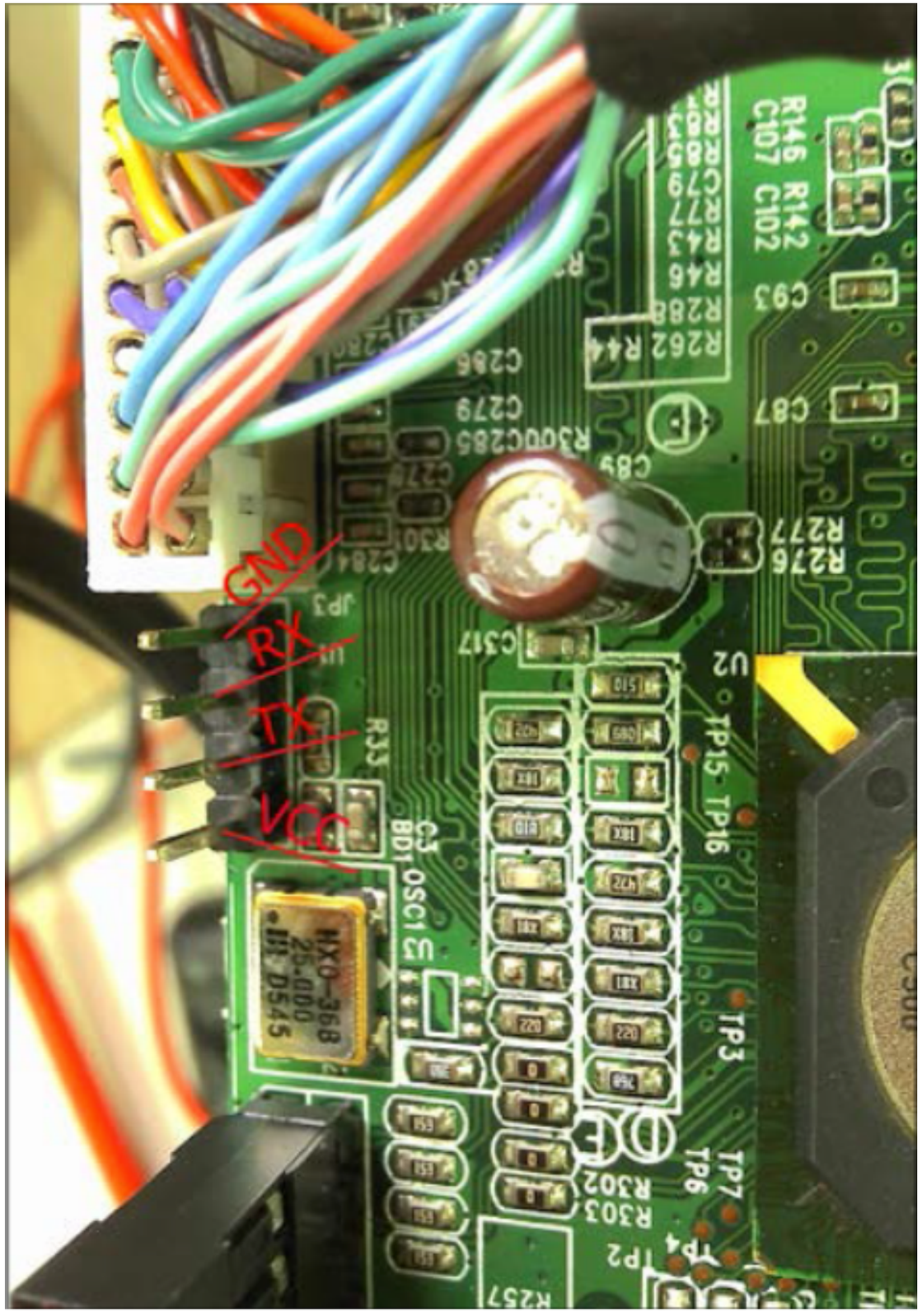
- 這時embedded system 再通電
  把探針一根固定放 GND 測試每根與第一根已知 （GND）
  相通電呀 發現當 1,4 腳位通電時3.3V或5V

OSSLab

- 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

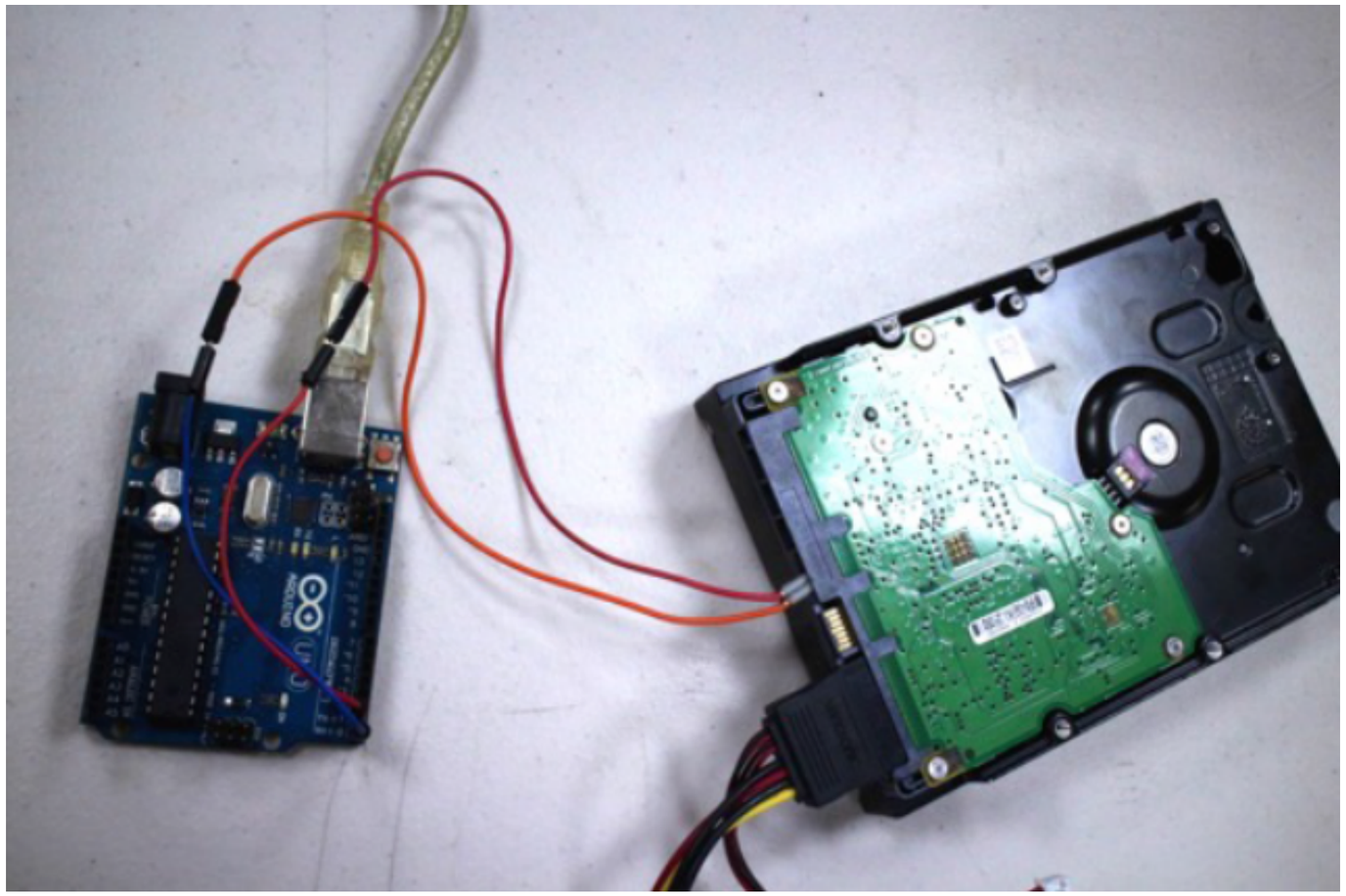


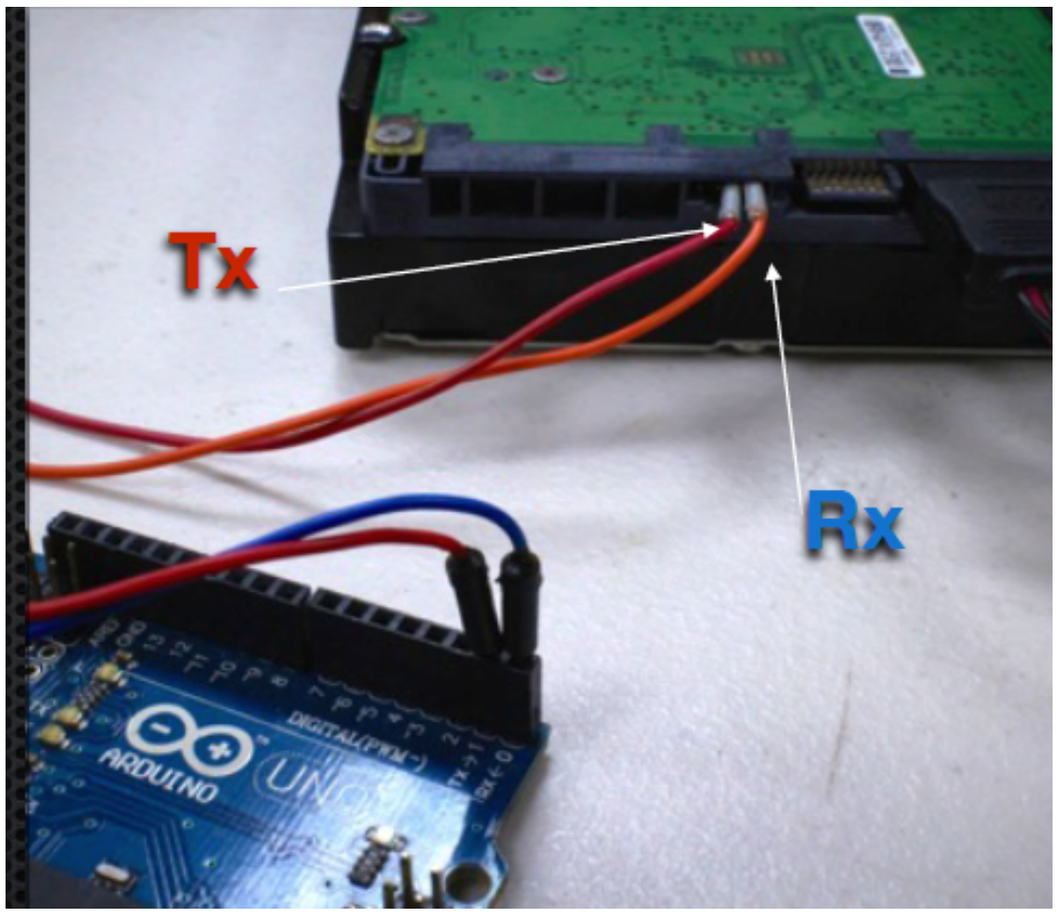
分析出腳位



OSSLab

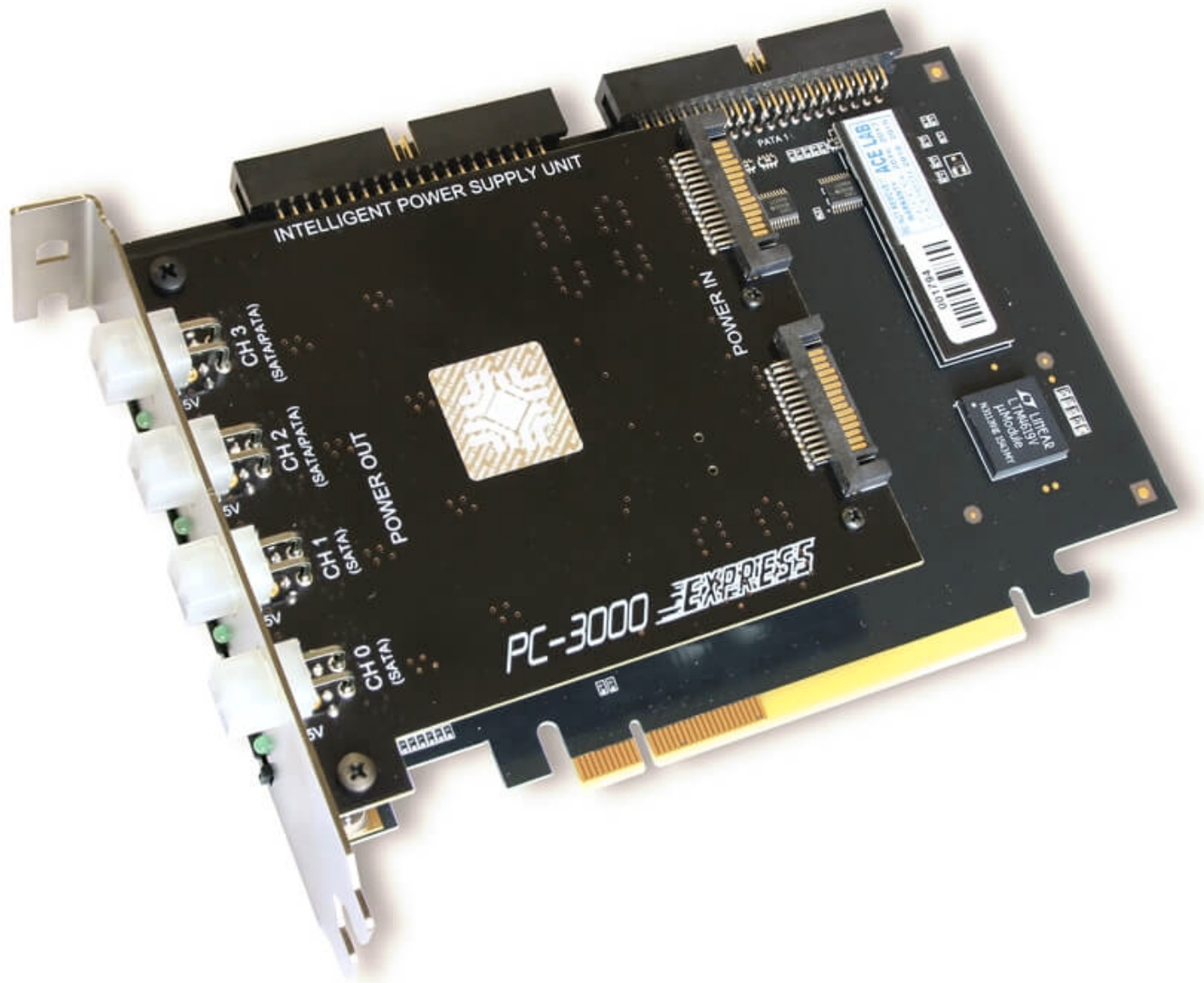
Seagate UART接線法





OSSLab

發出VSC與串口指令的設備



OSSLab

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.
CCCCCCCCCCCCCCC
File Descriptor FD37430A
File Size 00001000
Byte Offset 00000000
Bytes to write 00001000
F3 T>_
```

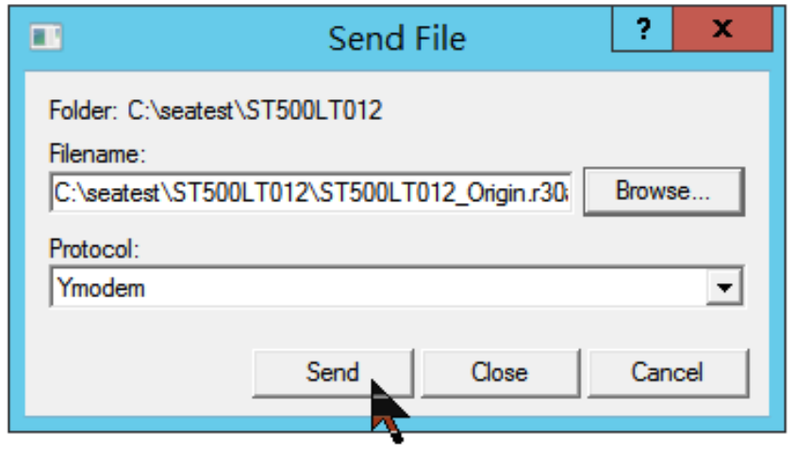
onnected 02:05:01 | Auto detect | 38400 8-N-1 | SCROLL | CAPS

OSSLab

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 T>
ASCII Diag mode

F3 T>
ASCII Diag mode

F3 T>w30a

File Volume 3
File ID 30A
File Copy Number 0
Start file transfer protocol in 60 seconds.
CCCCCCCCCCCCC_
```



OSSLab

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

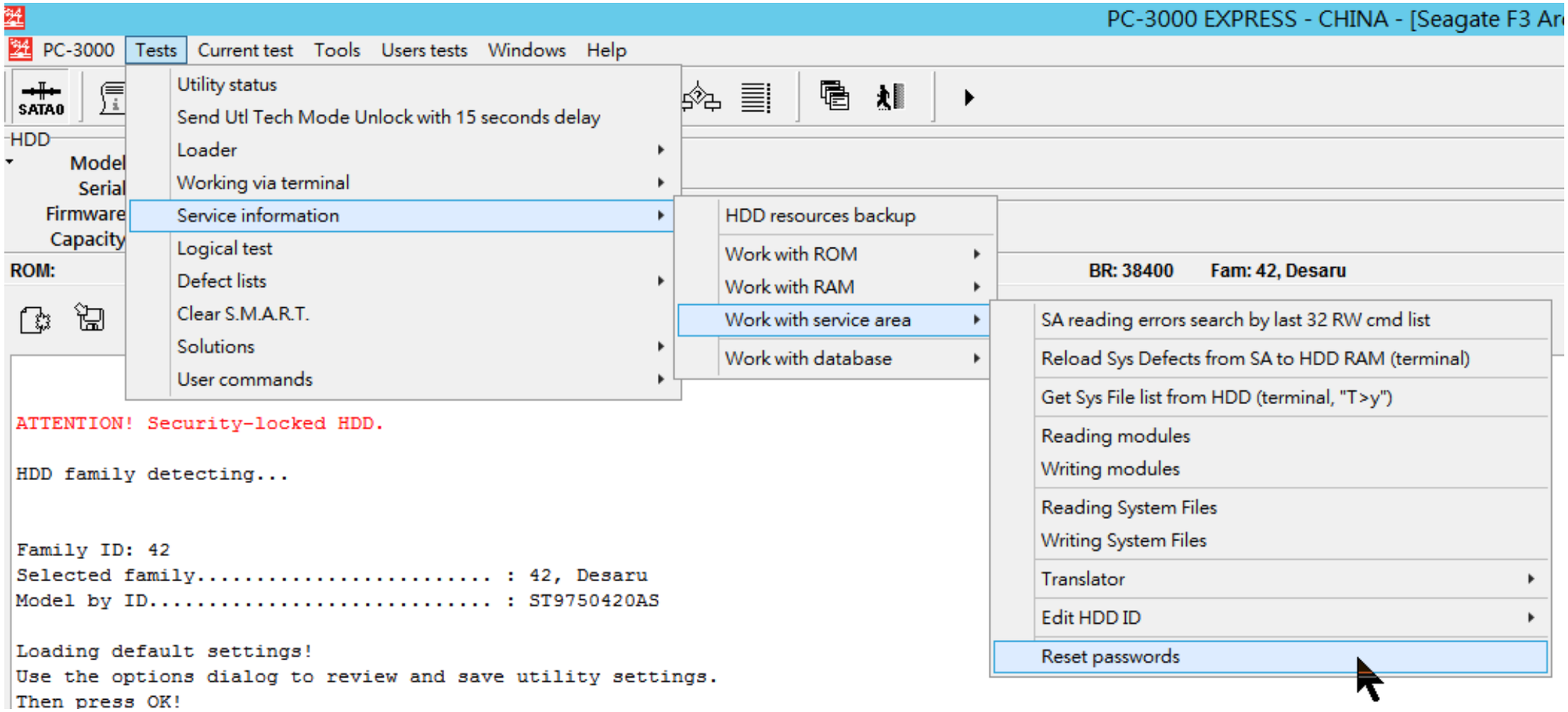
Module	Sys. file	Description
00		Defect list of SA
01	0x001A	Drive information file
02	0x0019	Performance parameter file
03	0x001B	P-List
04	0x003F	SAP (Servo Adaptive FParameters)
05	0x0300	Manufacturin information file
06	0x0001	RAP (Read Adaptives Parameters)
07	0x0208	CAP (Controller Adaptives Parameters)

OSSLab

把所有抓出的韌體區塊做比對

公開版簡報保留

看看專業怎做的



OSSLab

分析專業設備的方法

Offset | 0 1 2 3 4 5 6 7 8 9 A B C D E F | ANSI ASCII

```
00000000  ED FE 0D 90 FF FF 06 00  11 28 00 00 00 00 FF FF  íþ  ÿÿ   (    ÿÿ
00000010  FF 0F 00 00 00 00 00 00  00 00 30 60 38 3A 00 00  ÿ          0`8:
00000020  00 00 30 60 38 3A 00 00  00 00 30 60 38 3A 00 00    0`8:    0`8:
00000030  00 00 17 18 30 60 38 3A  00 00 00 00 00 00 00 00      0`8:
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 F0 60 A9       T   rUað`©
00000060  00 2B B4 52 60 ED ED 9E  09 AF 6D 03 23 77 91 0C    +´R`ííž ¯m #w'
00000070  71 D3 BA F1 CC E8 C8 B8  30 FF 72 55 61 F0 60 A9  qÓºñÌèÈ¸0ÿrUað`©
00000080  00 2B B4 52 60 ED ED 9E  09 AF 6D 03 23 77 91 0C    +´R`ííž ¯m #w'
00000090  71 D3 BA F1 CC E8 C8 B8  30 FF 01 40 04 00 06 20  qÓºñÌèÈ¸0ÿ @
000000A0  07 06 00 00 00 00 00 00  00 00 1A 60 02 00 07 00              `
000000B0  7F 00 30 60 38 3A 00 00  00 00 9F 79 15 00 00 00    0`8:    Ÿy
000000C0  00 20 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0  00 00 00 00 00 00 00 00  6B 74 29 7D 63 61 6B 74          kt)}cakt
000000E0  09 BC 63 61 0E 40 0A 40  00 40 00 00 00 00 00 D0    ¼ca @ @ @      Ð
000000F0  FF 3F FF 3F 00 00 27 01  FF FF FF 0F 30 60 38 3A  ÿ?ÿ?  '  ÿÿÿ 0`8:
00000100  00 00 00 00 06 0F 48 00  40 00 A5 DC AC 59 AC 59        H @ ¥Ü¬Y¬Y
00000110  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000120  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000130  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000140  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000150  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
```

Page 1 of 12 | Offset: 0

ST500LT012_WC30CD_NBF_WD_Reset.raw

Offset | 0 1 2 3 4 5 6 7 8 9 A B C D E F | ANSI ASCII

```
00000000  ED FE 0D 90 FF FF 06 00  11 28 00 00 00 00 FF FF  íþ  ÿÿ   (    ÿÿ
00000010  FF 0F 00 00 00 00 00 00  00 00 30 60 38 3A 00 00  ÿ          0`8:
00000020  00 00 30 60 38 3A 00 00  00 00 30 60 38 3A 00 00    0`8:    0`8:
00000030  00 00 17 18 30 60 38 3A  00 00 00 00 00 00 00 00      0`8:
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 72 55 61 F0 60 A9       T   rUað`©
00000060  00 2B B4 52 60 ED ED 9E  09 AF 6D 03 23 77 91 0C    +´R`ííž ¯m #w'
00000070  71 D3 BA F1 CC E8 C8 B8  30 FF 72 55 61 F0 60 A9  qÓºñÌèÈ¸0ÿrUað`©
00000080  00 2B B4 52 60 ED ED 9E  09 AF 6D 03 23 77 91 0C    +´R`ííž ¯m #w'
00000090  71 D3 BA F1 CC E8 C8 B8  30 FF 01 40 00 00 06 20  qÓºñÌèÈ¸0ÿ @
000000A0  07 06 00 00 00 00 00 00  00 00 1A 60 02 00 07 00              `
000000B0  7F 00 30 60 38 3A 00 00  00 00 9F 79 15 00 00 00    0`8:    Ÿy
000000C0  00 20 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0  00 00 00 00 00 00 00 00  6B 74 29 7D 63 61 69 74          kt)}cait
000000E0  09 BC 63 61 0E 40 0A 40  00 40 00 00 00 00 00 D0    ¼ca @ @ @      Ð
000000F0  FF 3F FF 3F 00 00 21 00  FF FF FF 0F 30 60 38 3A  ÿ?ÿ?  !  ÿÿÿ 0`8:
00000100  00 00 00 00 06 0F 48 00  40 00 A5 E5 AC 59 AC 59        H @ ¥å¬Y¬Y
00000110  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000120  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000130  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000140  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
00000150  AC 59 AC 59 AC 59 AC 59  AC 59 AC 59 AC 59 AC 59  ¬Y¬Y¬Y¬Y¬Y¬Y¬Y¬Y
```


OSSLab

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

OSSLab

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硬體
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

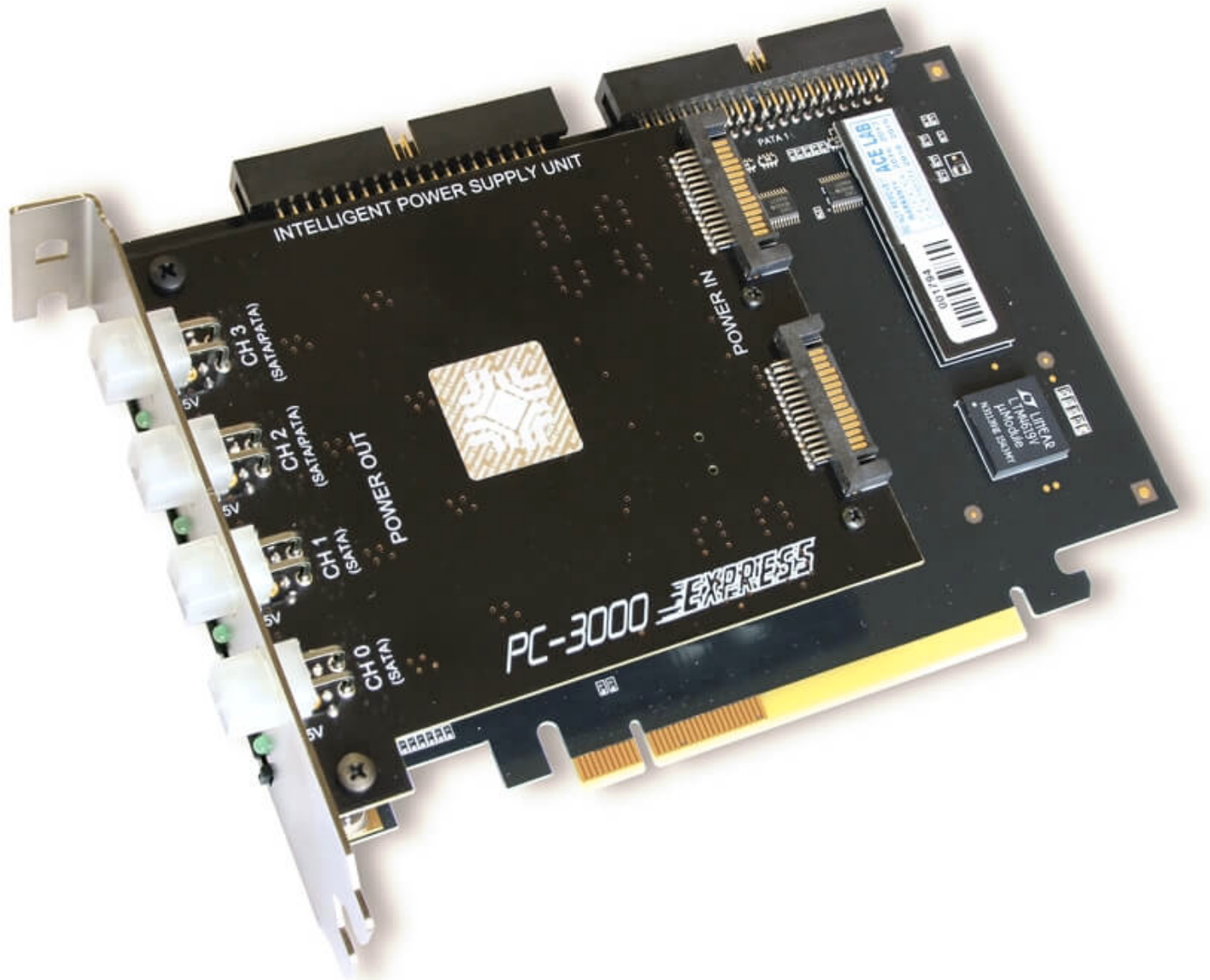
一.工廠內部軟體

二.韌體升級軟體

三.非官方資料救援設備硬體與軟體

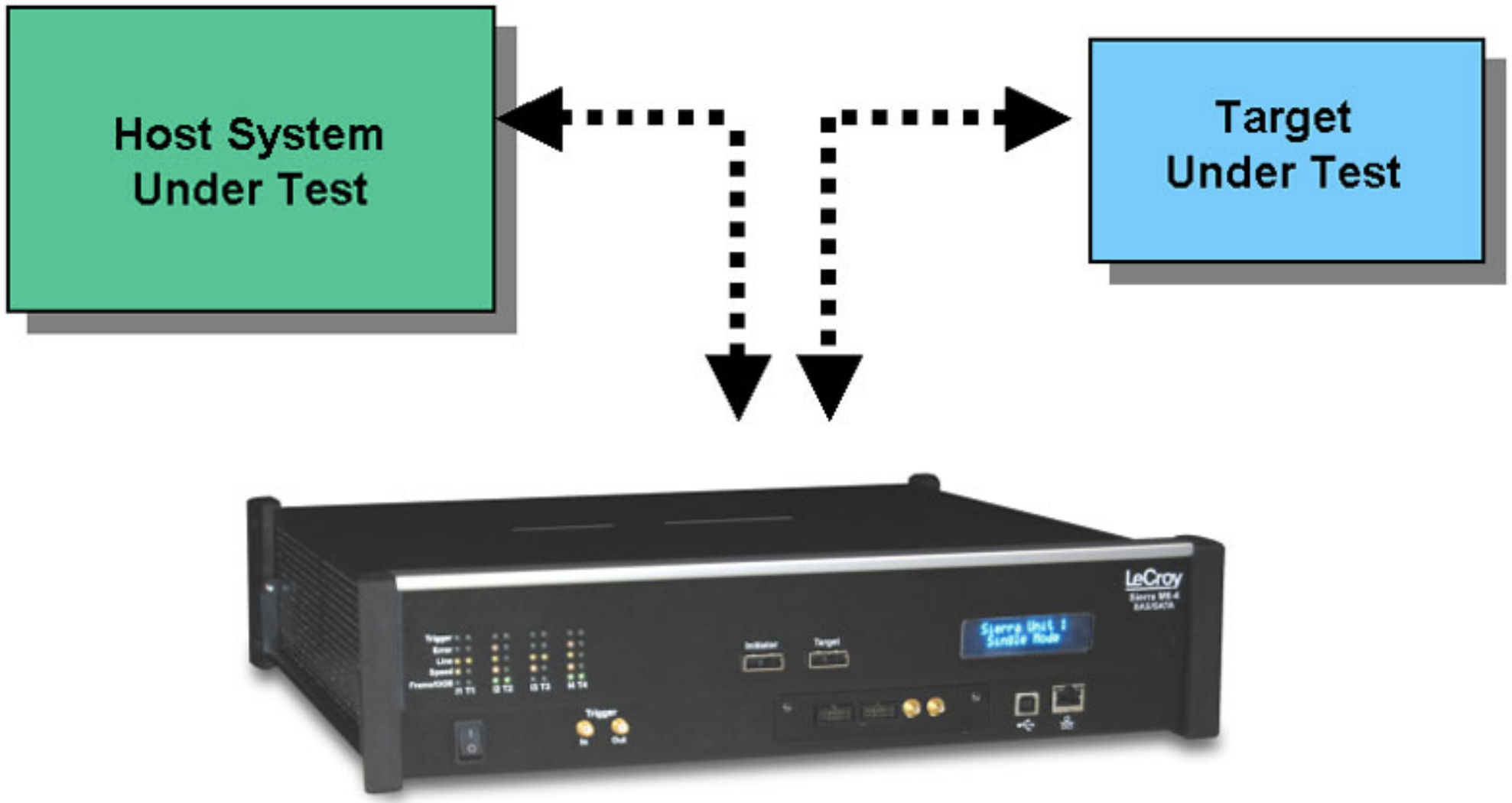
OSSLab

發出VSC的非原廠硬體



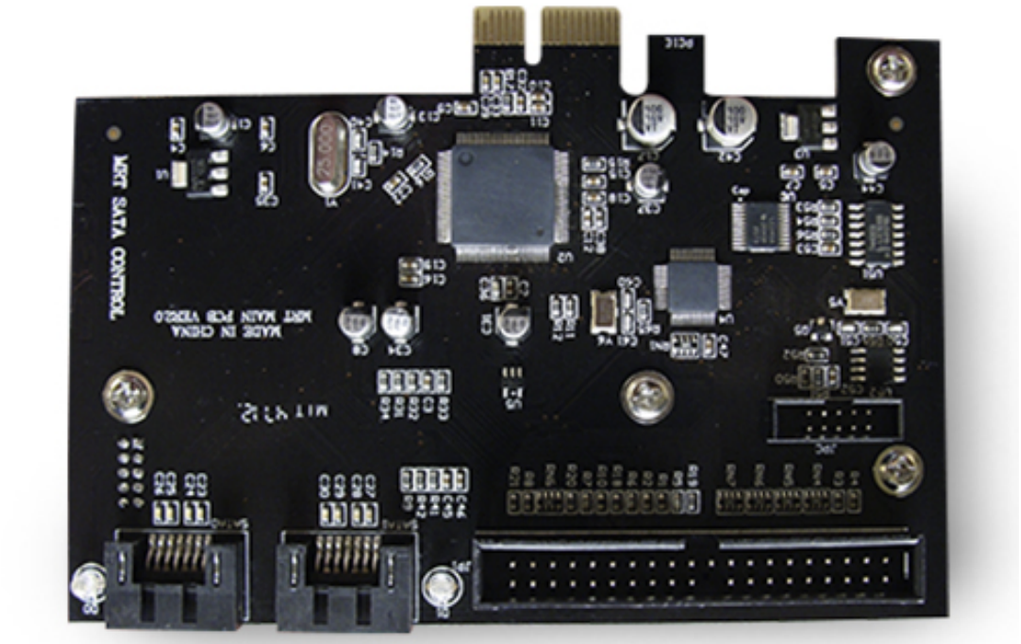
OSSLab

SATA 邏輯分析儀



OSSLab

資安硬體界“資源共享”



OSSLab

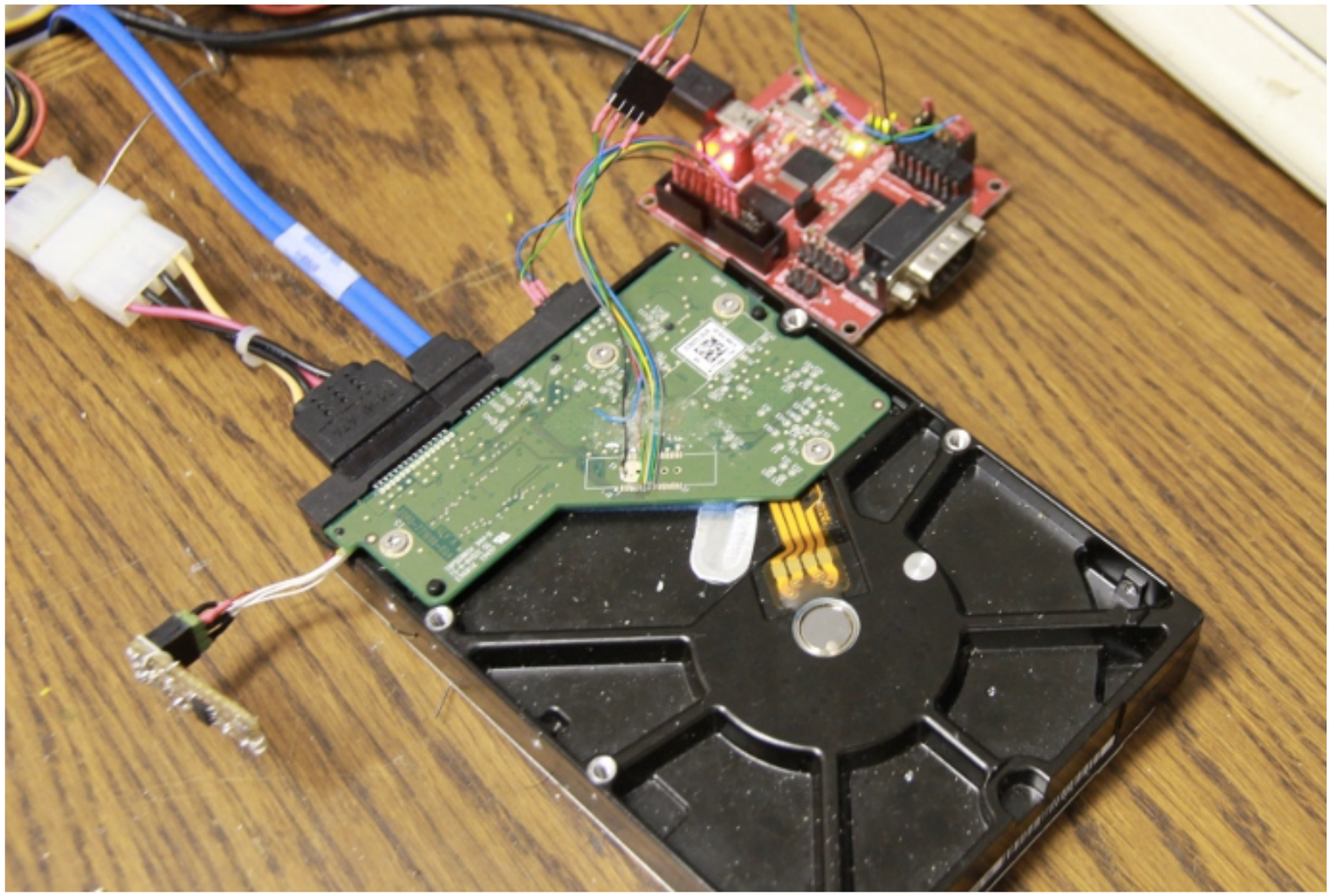
逆向工程靜態分析

公開版簡報保留

OSSLab

使用JTAG動態反組譯

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



OSSLab

窮舉Fuzzer指令集

公開版簡報保留

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)-'
&>
(1Ah)-TCG Serial Port Disabled
&>
(1Ah)-TCG Serial Port Disabled
&>
(1Ah)-TCG Serial Port Disabled
```

解鎖前, Serial Port被關閉

```
Tech Unlock Handshake: 0x1CEF53D8
Reply:
```

OSSLab

```
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

OSSLab

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

真的有後門嗎?

有後門指令,或是工廠指令實現破解硬碟安全系統

至於使用工廠指令集把木馬隱藏在硬碟 SSD 韌體區

目前實現上有很大難度.

難度其實在於引導程式碼 .

OSSLab

Http://www.osslab.com.tw

應用與原理必須相結合

Q&A