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

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

OSSLab

儲存裝置上的嵌入式架構

CPU Core ＋RAM

ROM

碟片上的韌體架構

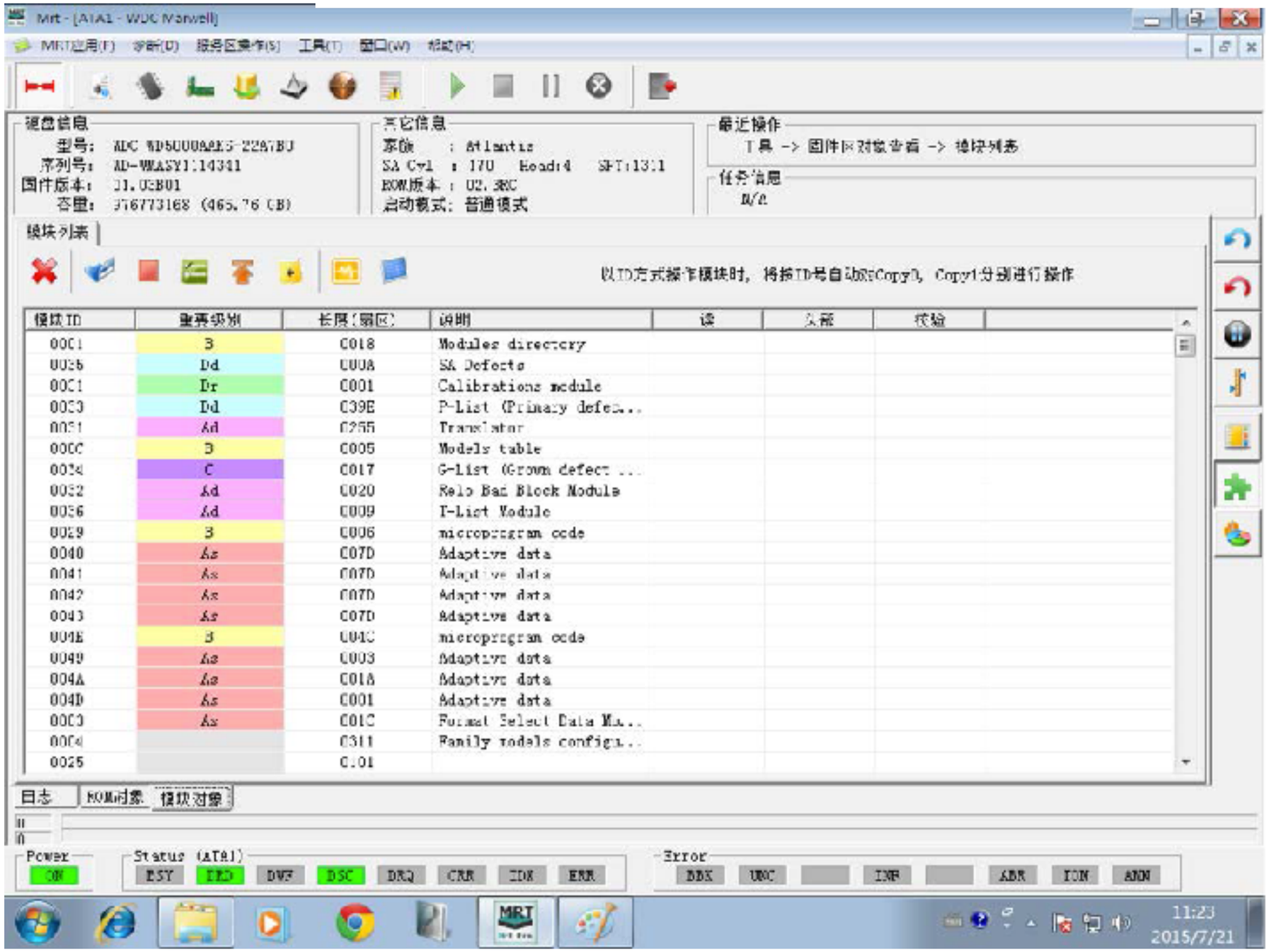
OSSLab

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 embedd system 不同的是儲存韌體地方會二個位置ROM跟碟片

OSSLab

WD 模塊列表



OSSLab

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 重要模塊一丟失 資料一去不復返

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

OSSLab

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 differentlyn 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

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

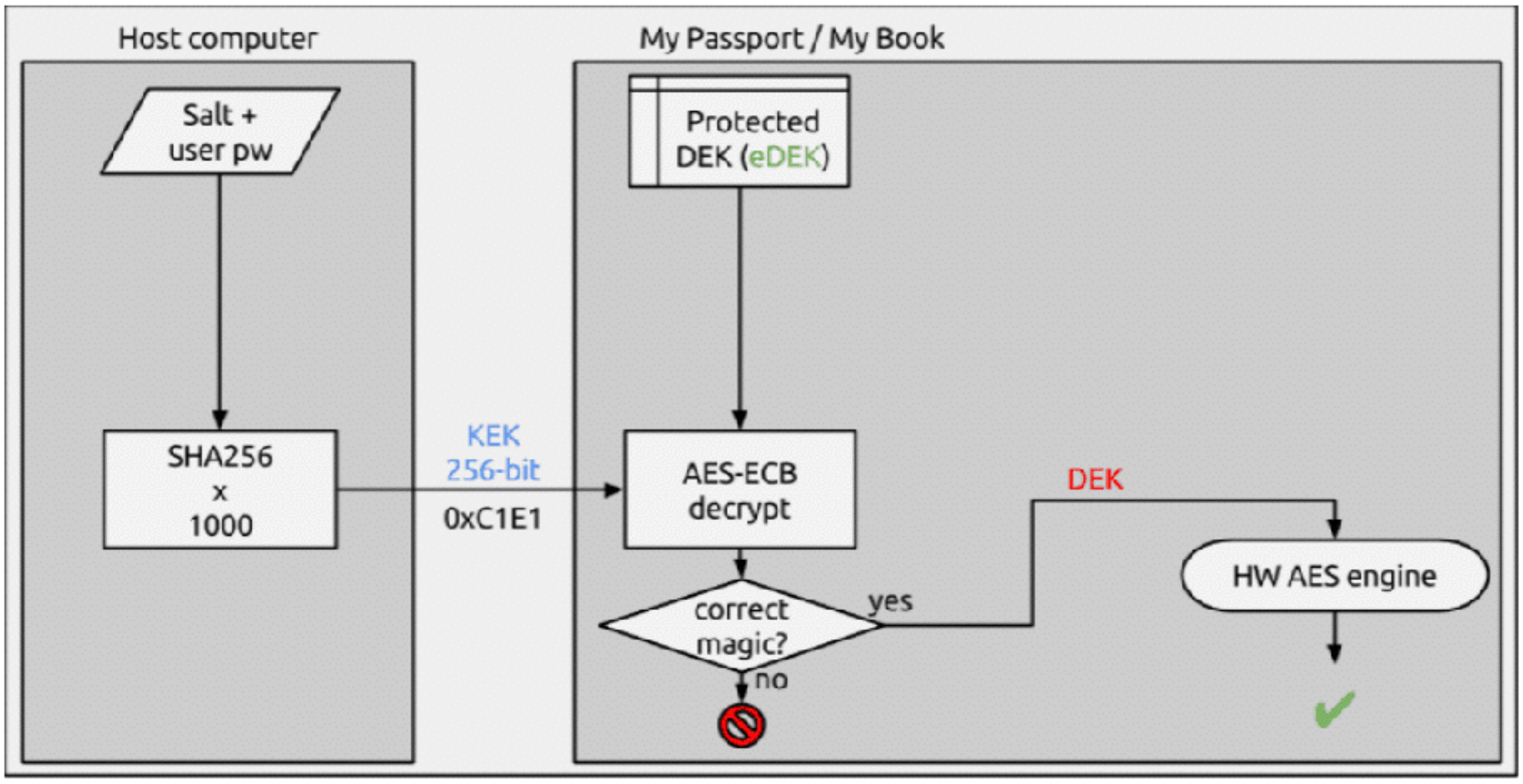
ATA 加密

OSSLab


My Passport
1.0TB
WD10JMVW
Not For Resale
5VDC : 0.55A
DCX : KA14J3TGH
DCM : SBKTJBB
DATE: 23 MAY 2013
WWN:50014EE6037D1337
USB
Product of Malaysia
S/N : WX51E33KHC46
MDL : WD10JMVW – 11AJGS1
U.S. Patents: 6178056, 595619F, 6289484, 6263459

OSSLab

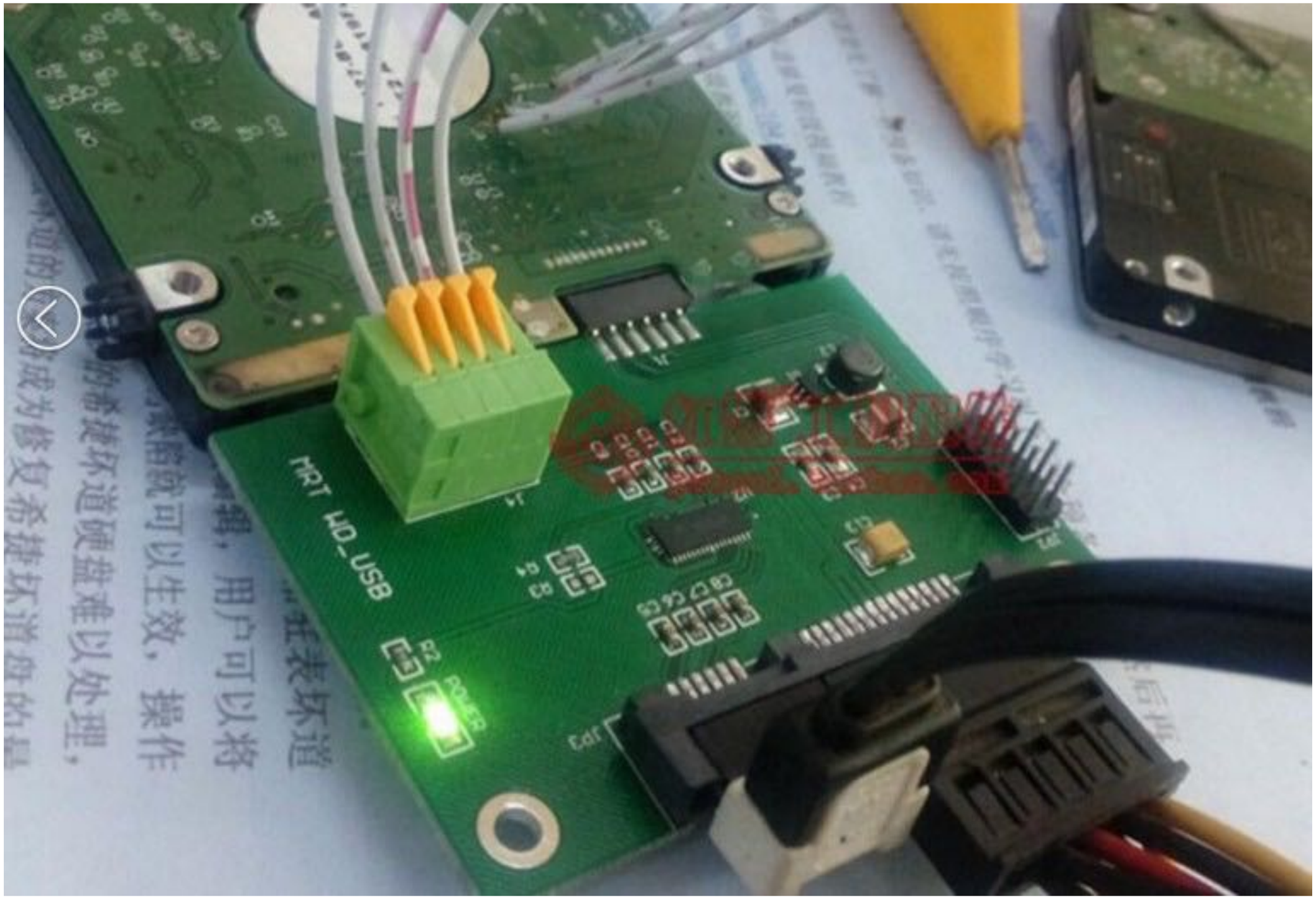
AES 加密



OSSLab

OSSLab

OSSLab


MRT MD_USB
POWER
J3

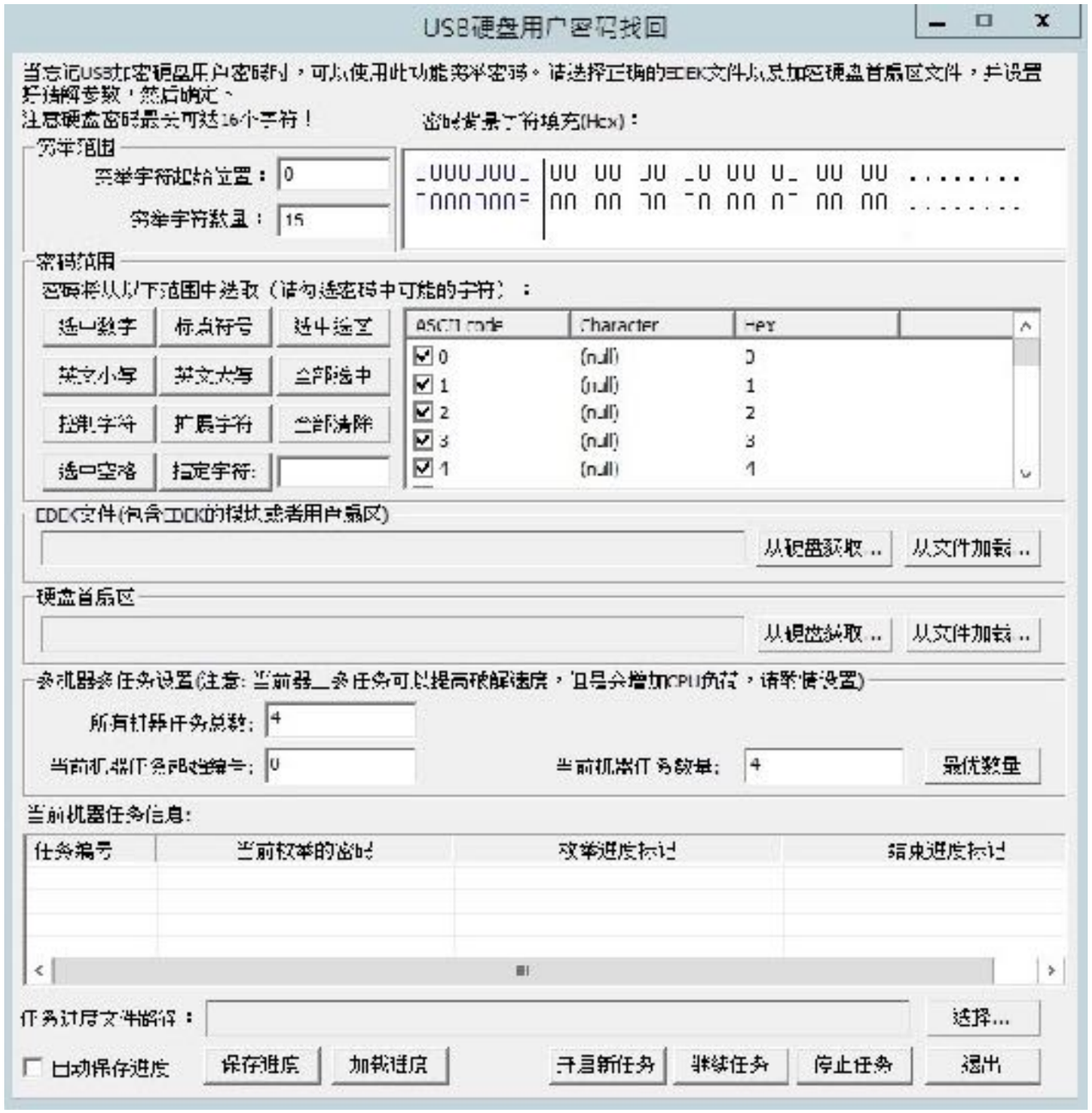
OSSLab

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  ..¯.ƒî.Ðès.....
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)

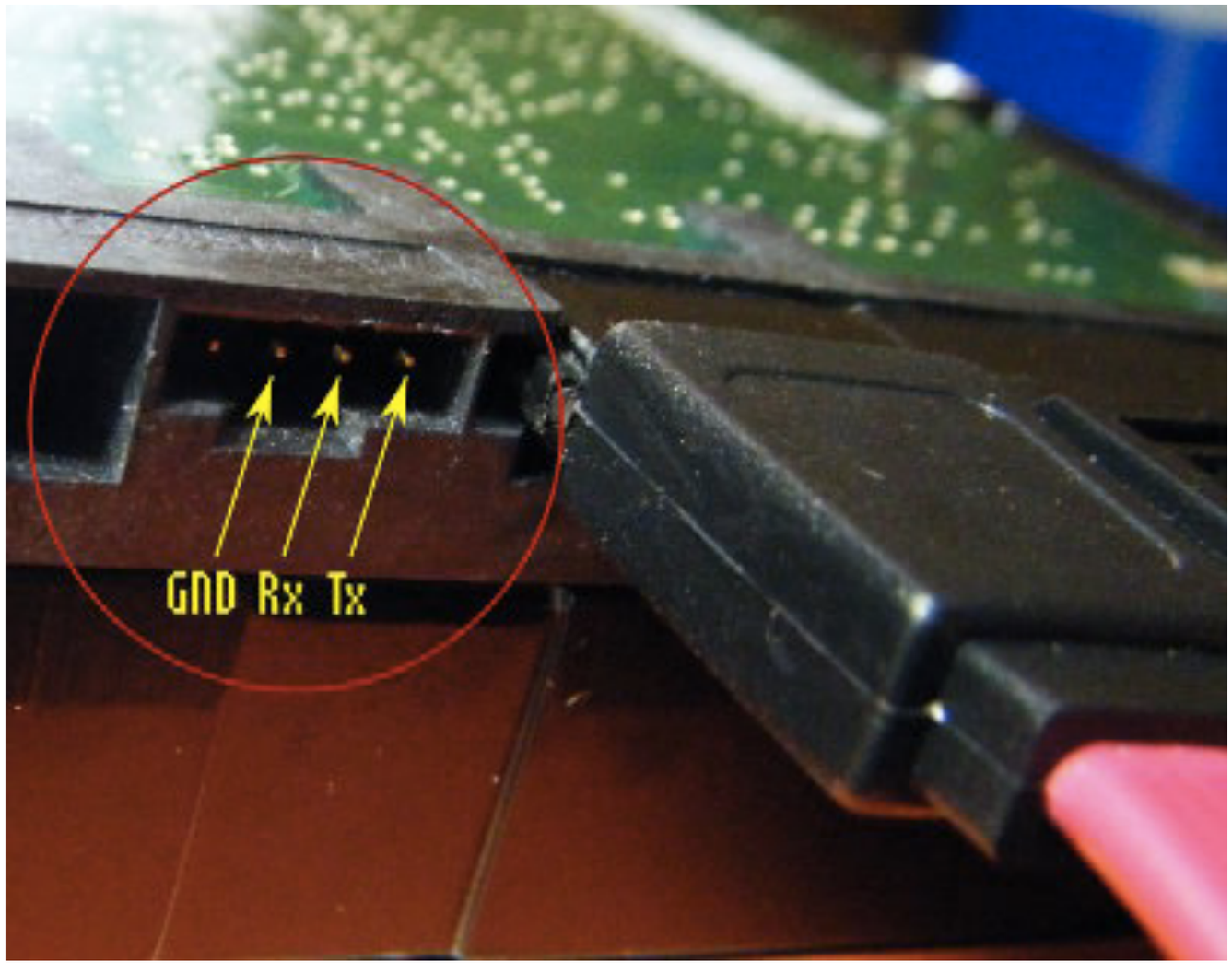
Seagate
F3 Serial Port Diagnostics

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

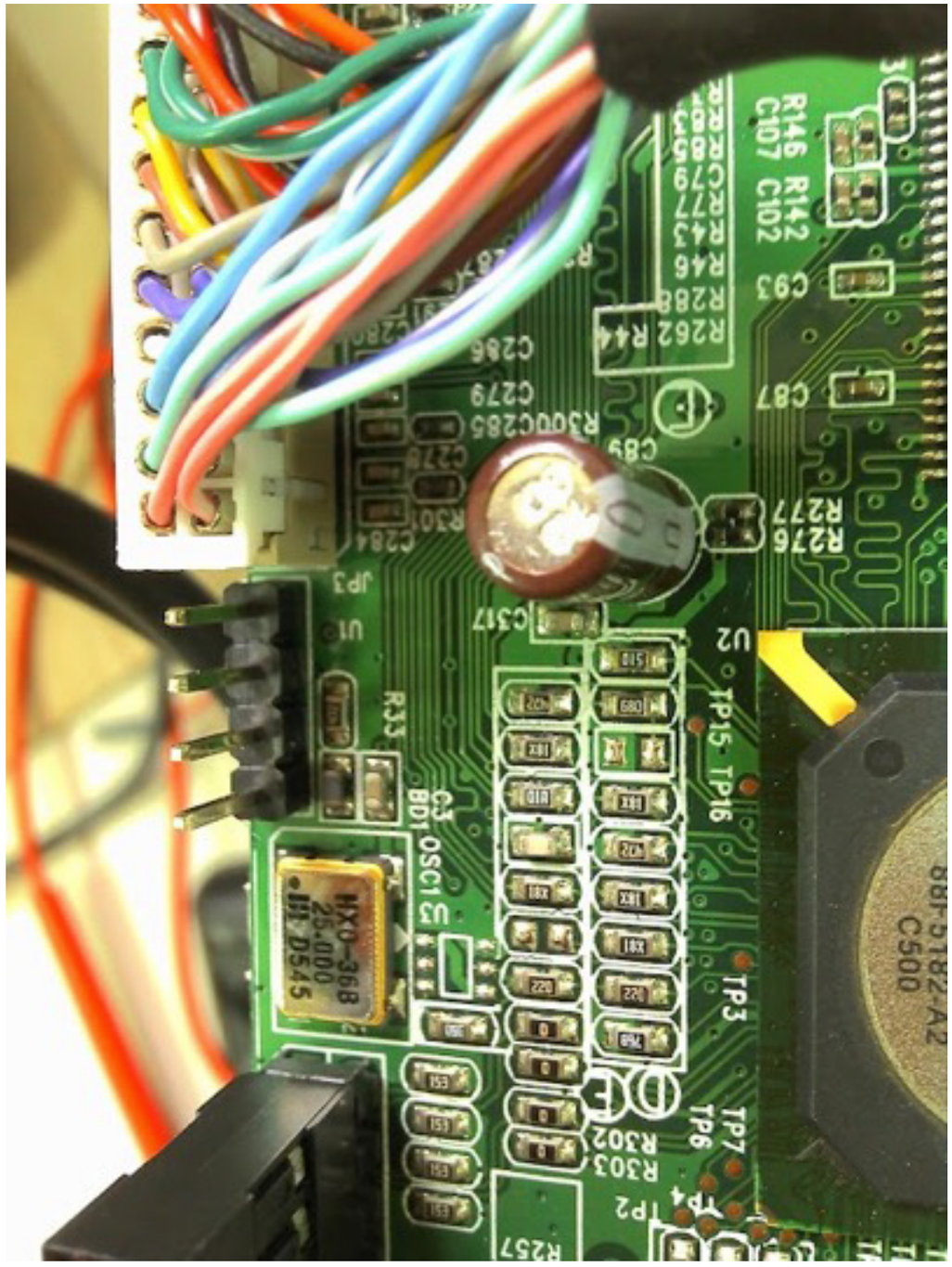
Serial TTL (UART)通訊

- 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

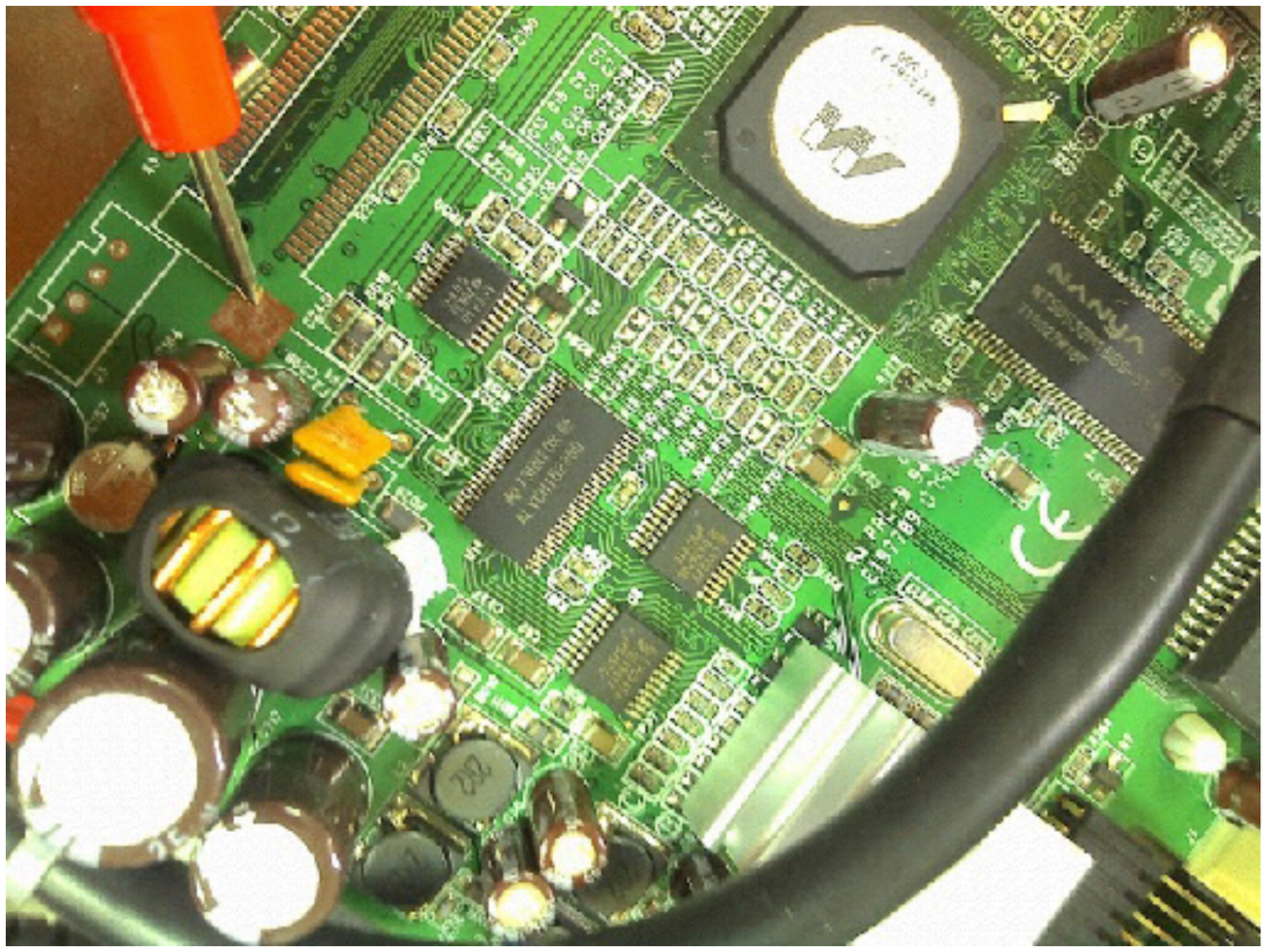
OSSLab

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)

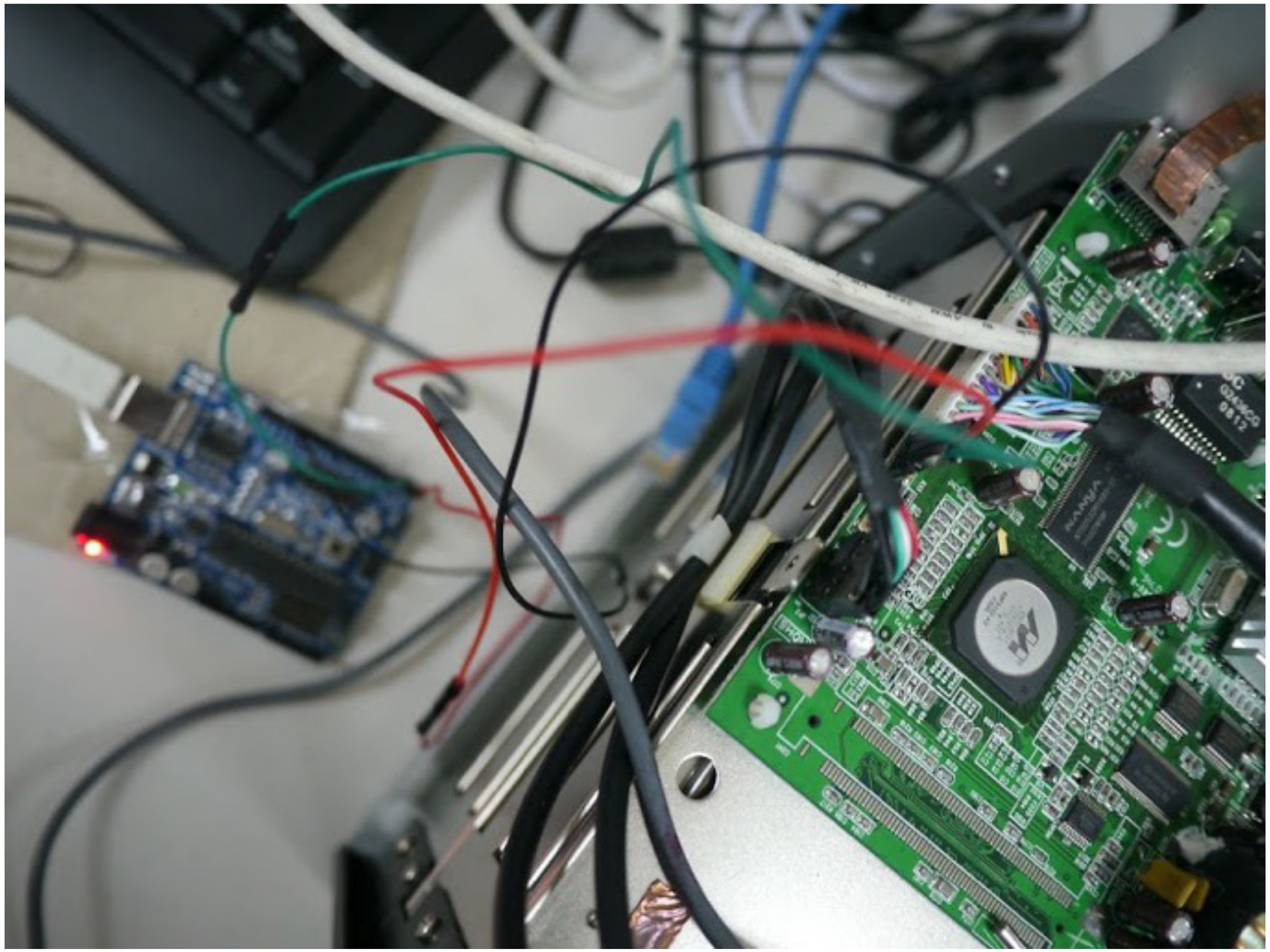
- 另外一邊探針 則每個Pin都試, 發現第一根有跟接地點導通, 會翁鳴。
  因此第一根為GND



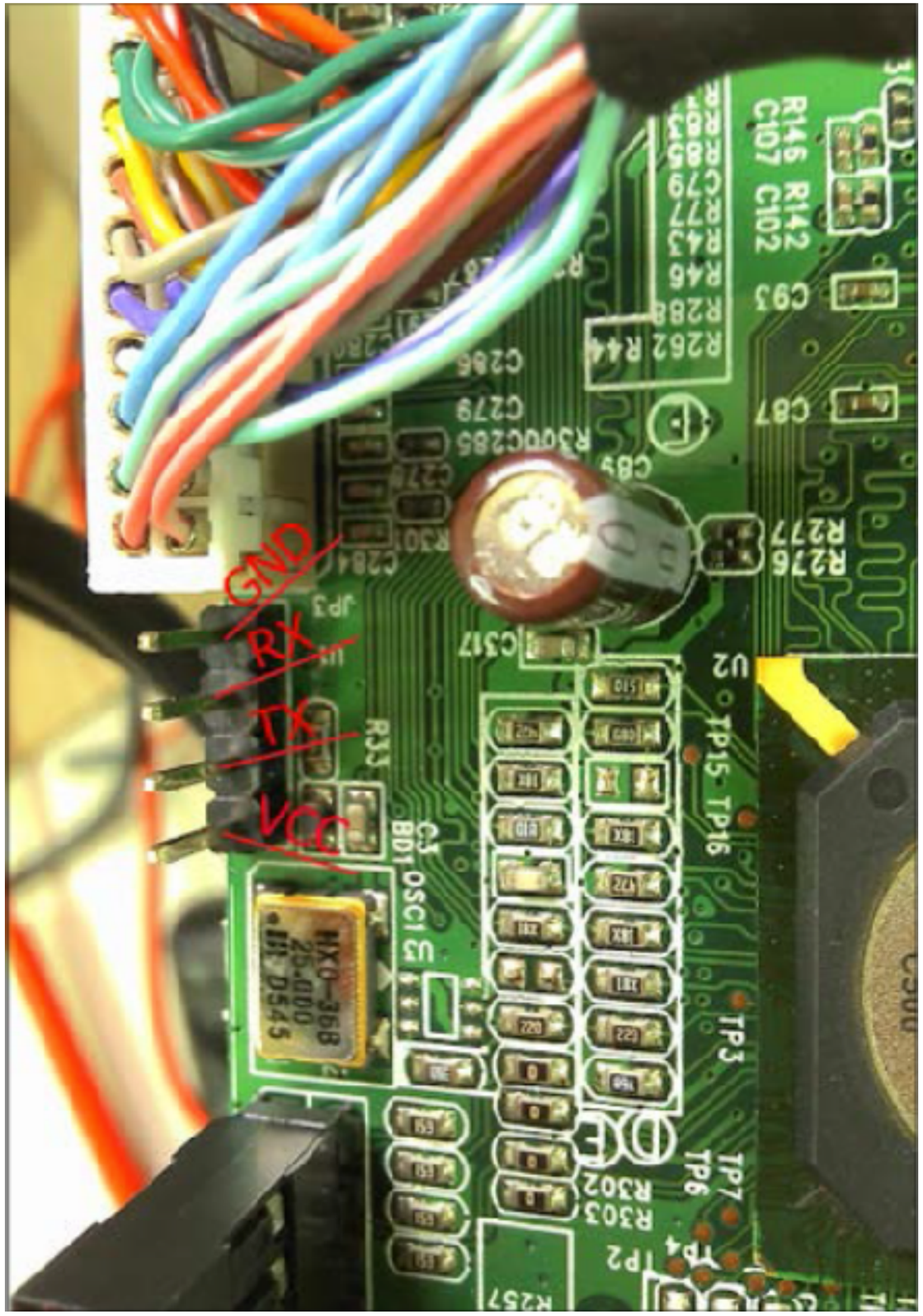
OSSLab

- 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

- 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

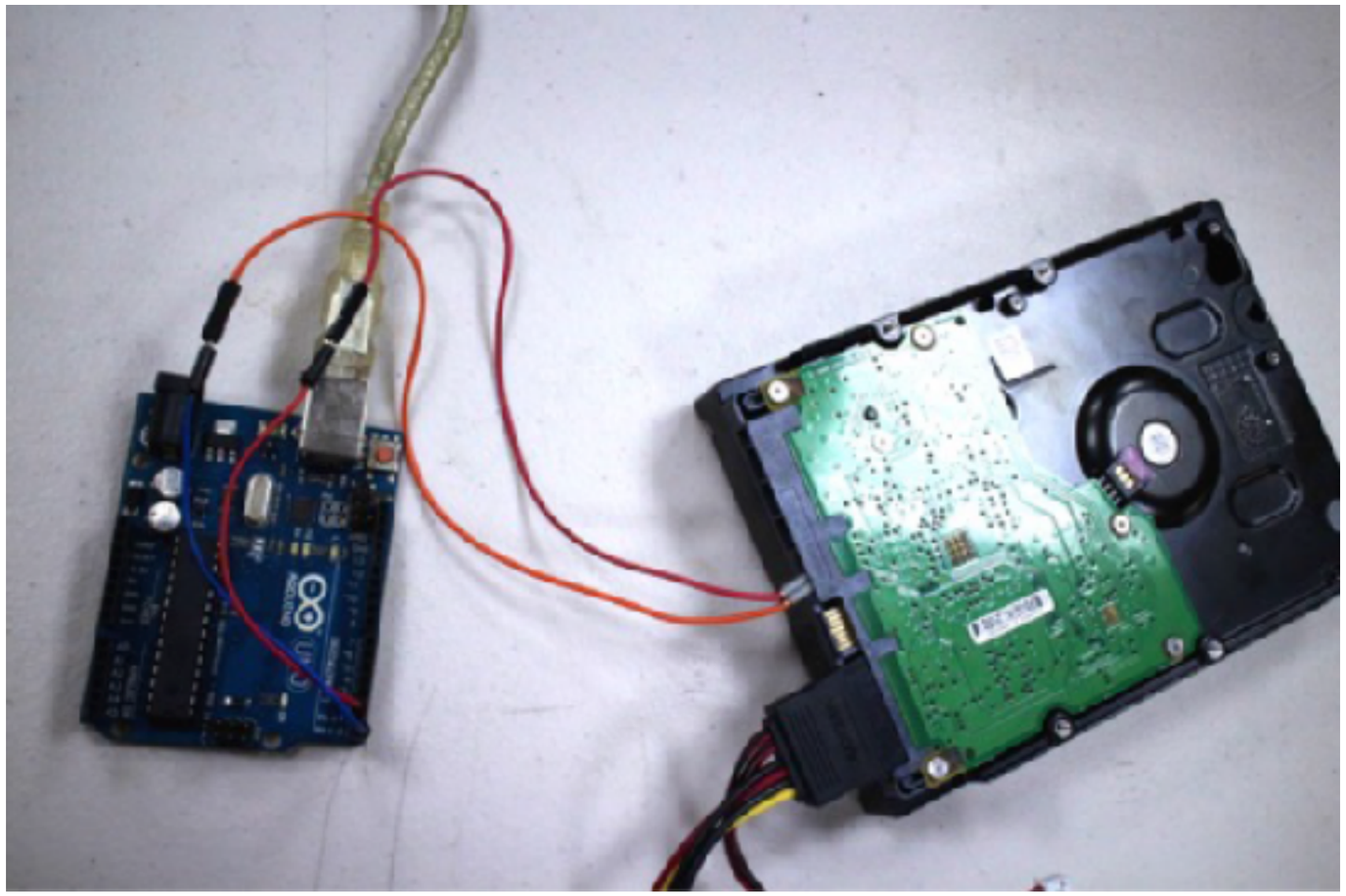


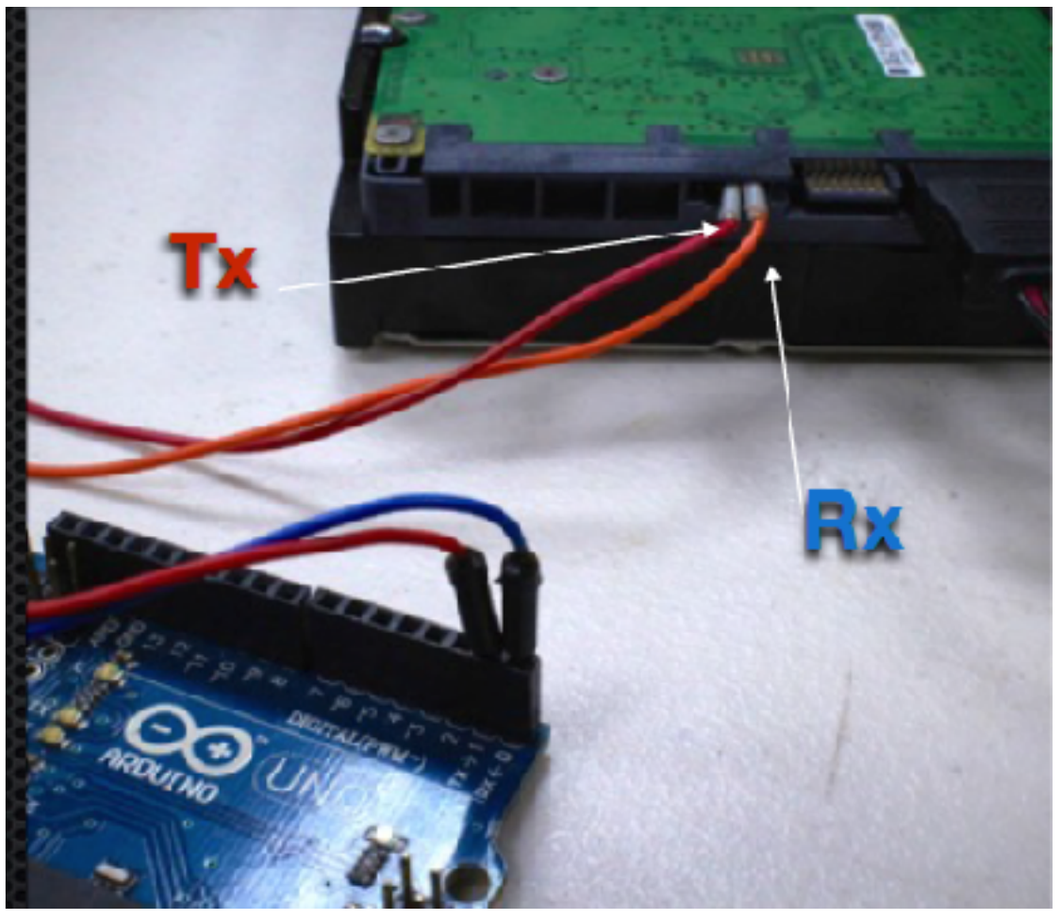
分析出腳位



OSSLab

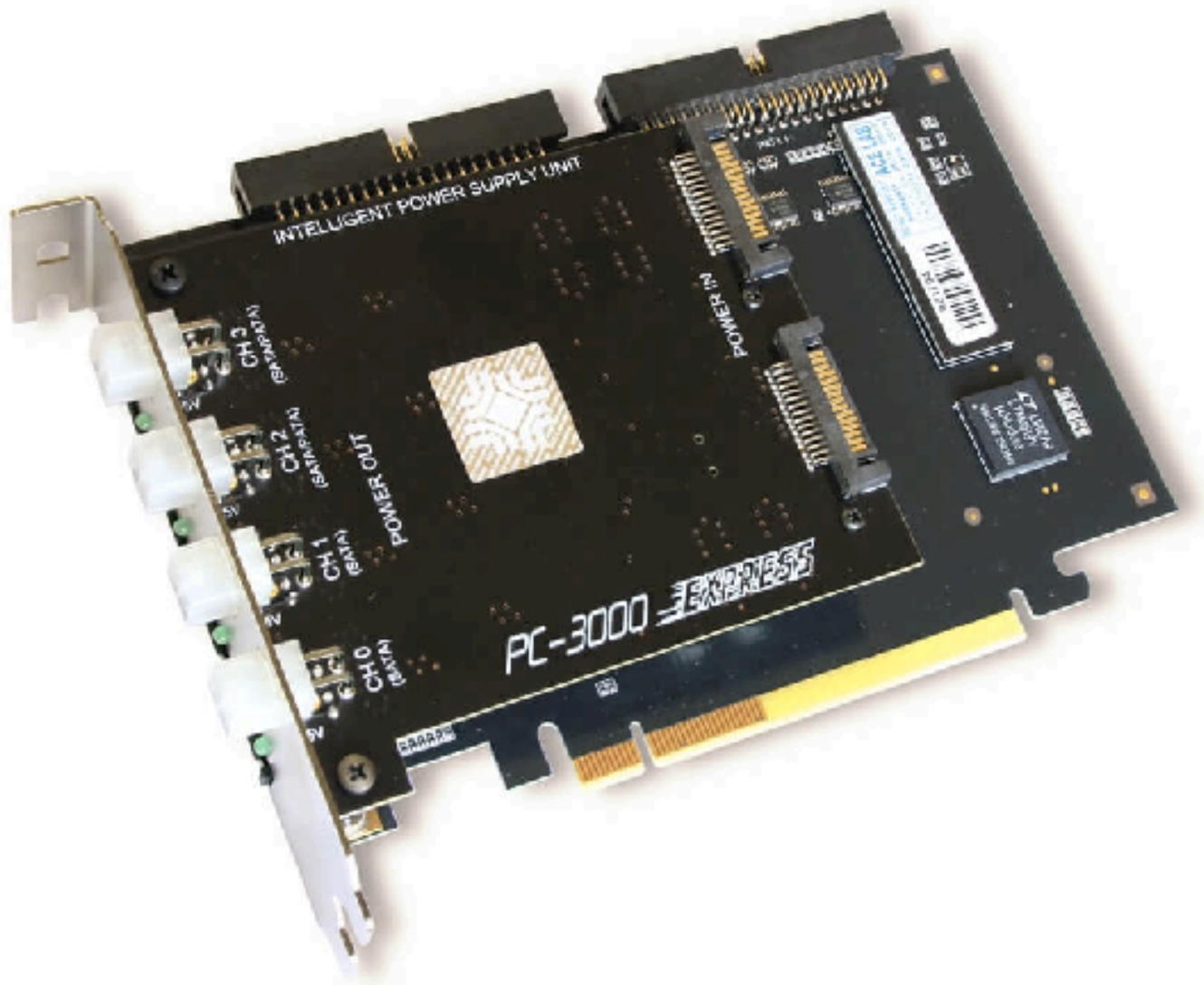
Seagate UART接線法





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：

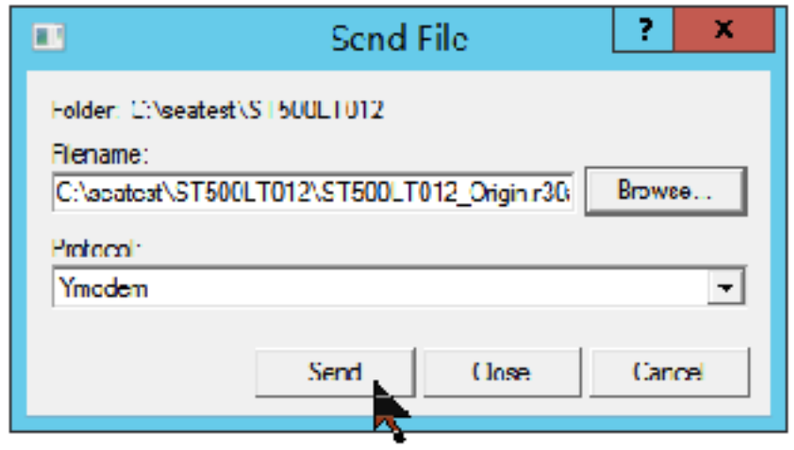
r 為讀取硬碟韌體系統文件

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



OSSLab

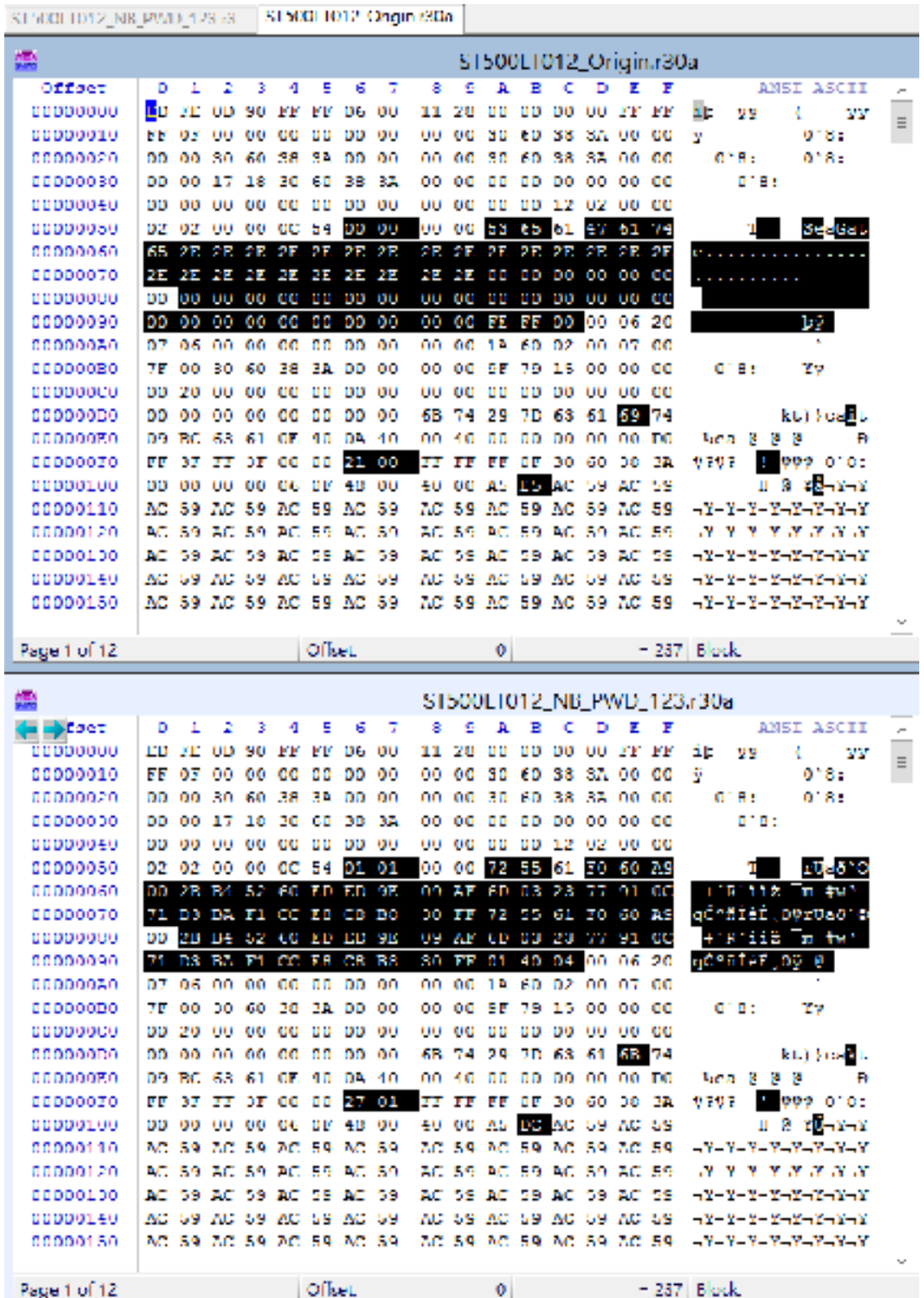
抓取所有硬碟韌體文件

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

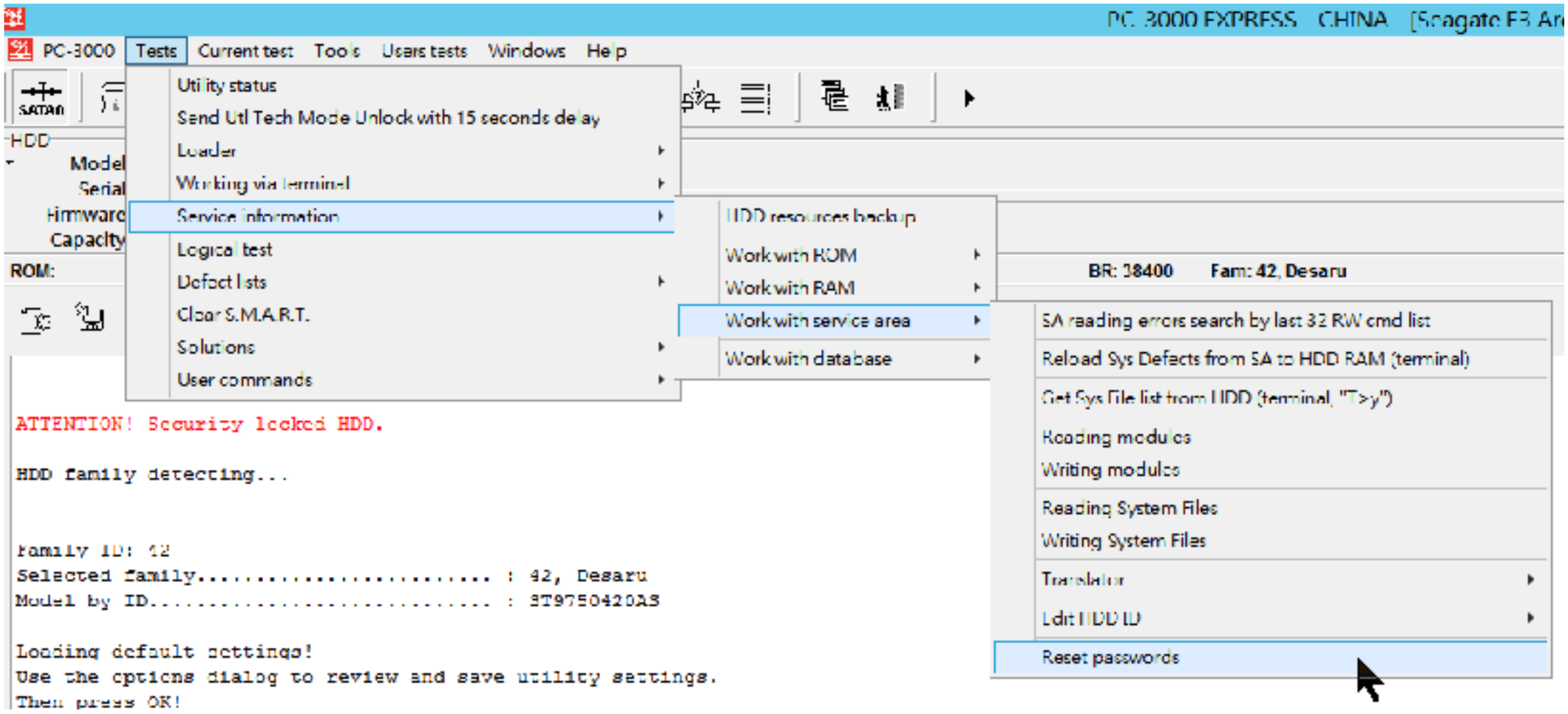
把所有抓出的韌體區塊做比對



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

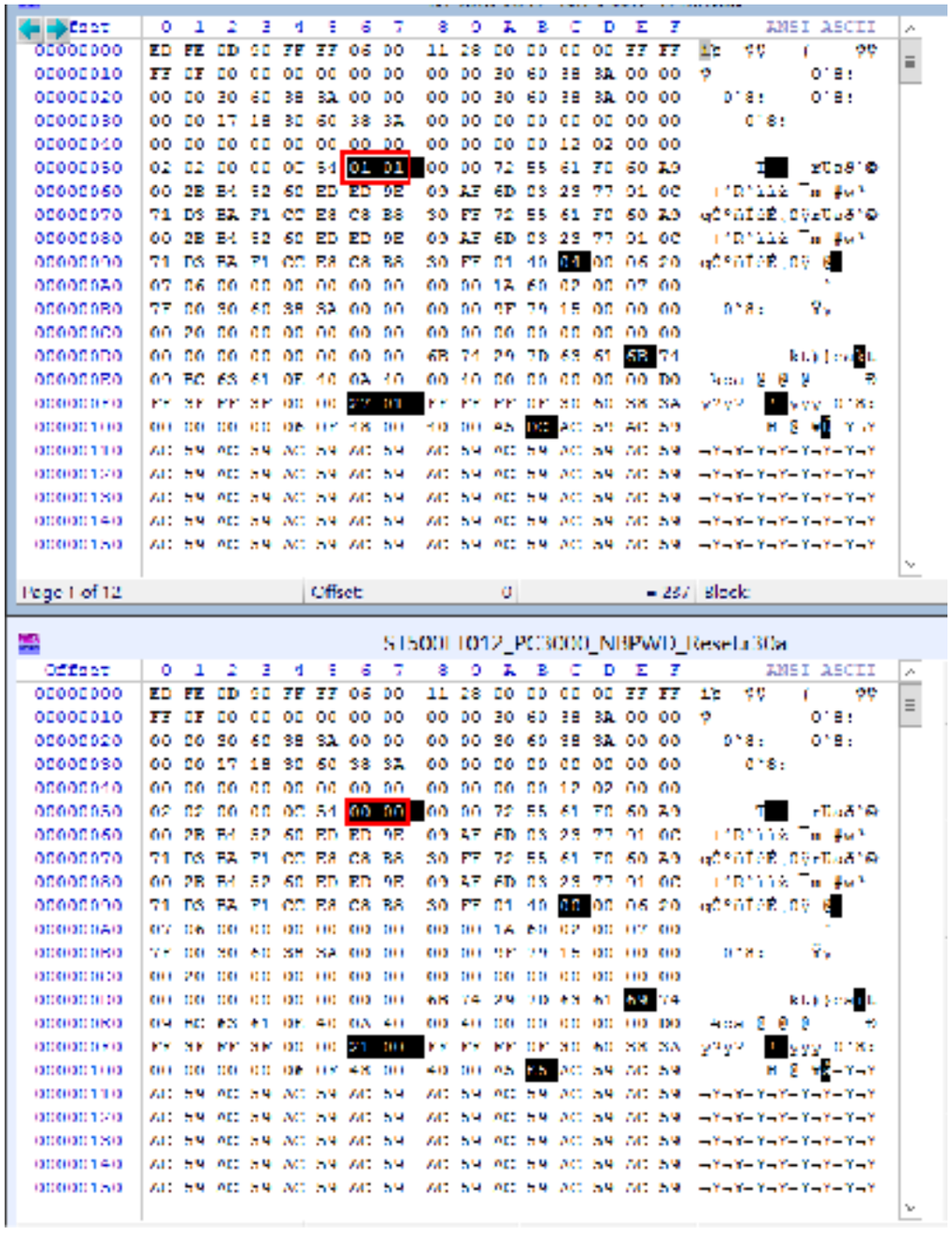
OSSLab

看看專業怎做的



OSSLab

分析專業設備的方法



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

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

OSSLab

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

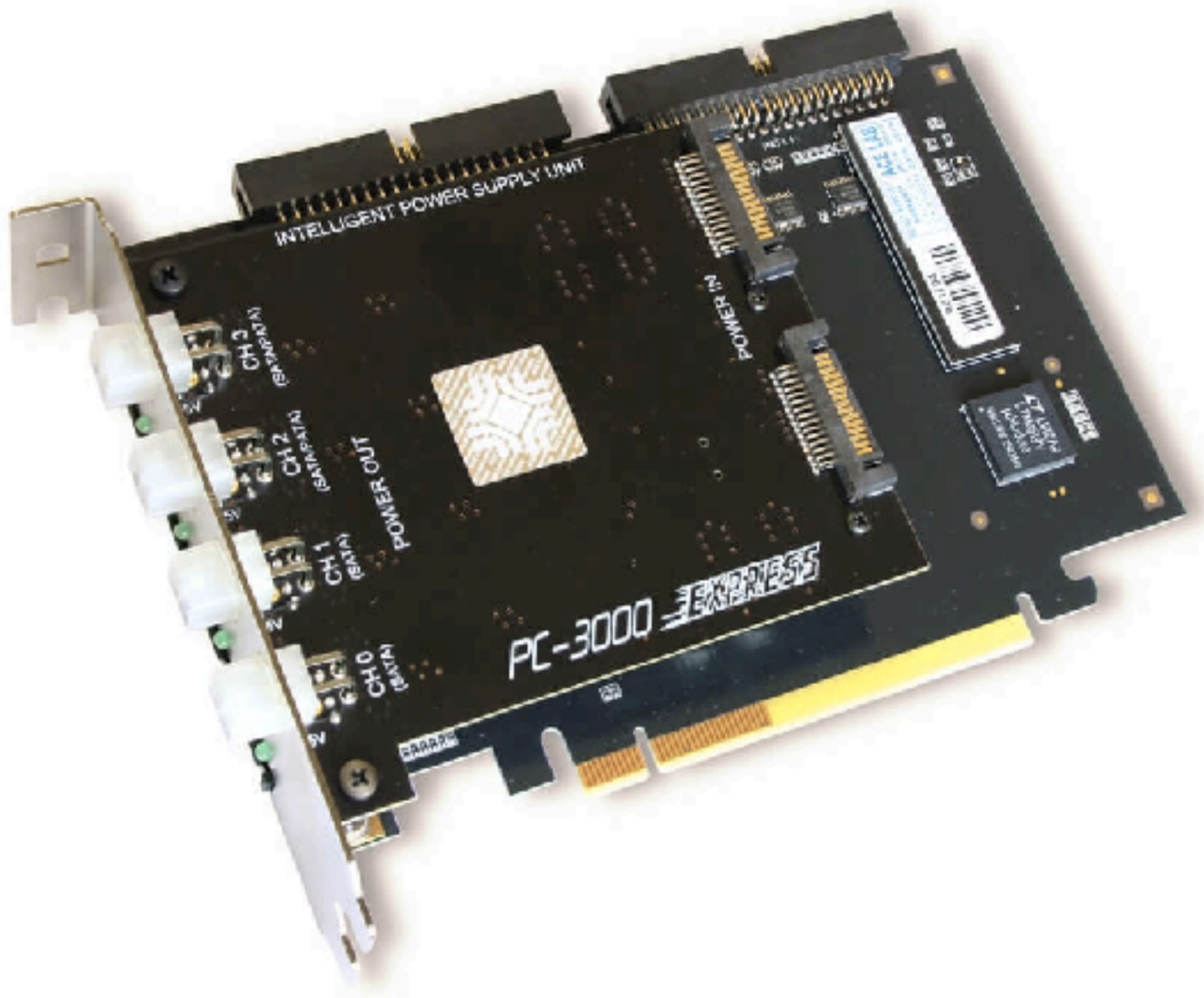
一.工廠內部軟體

二.韌體升級軟體

三.非官方資料救援設備硬體與軟體

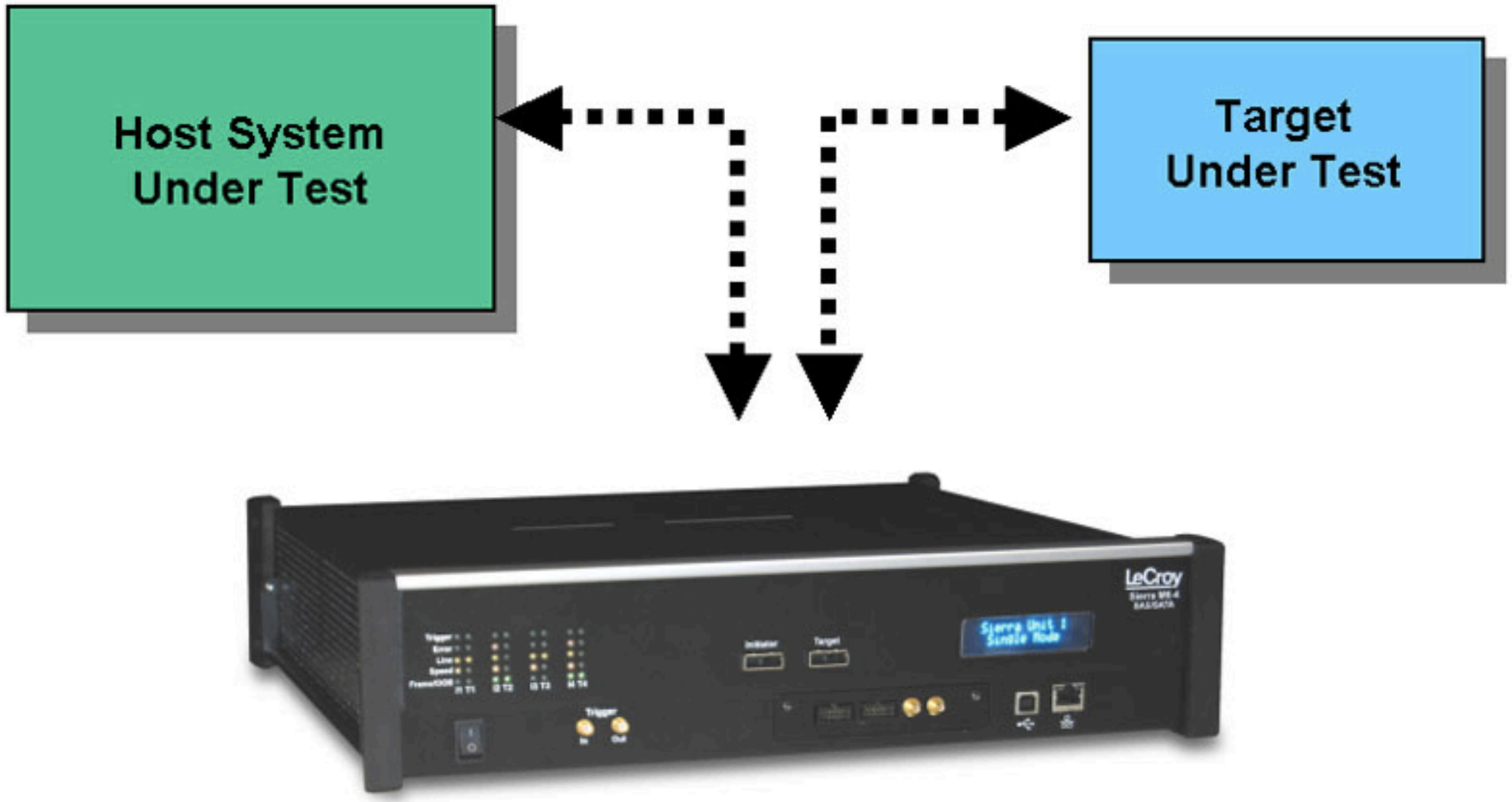
OSSLab

發出VSC的非原廠硬體



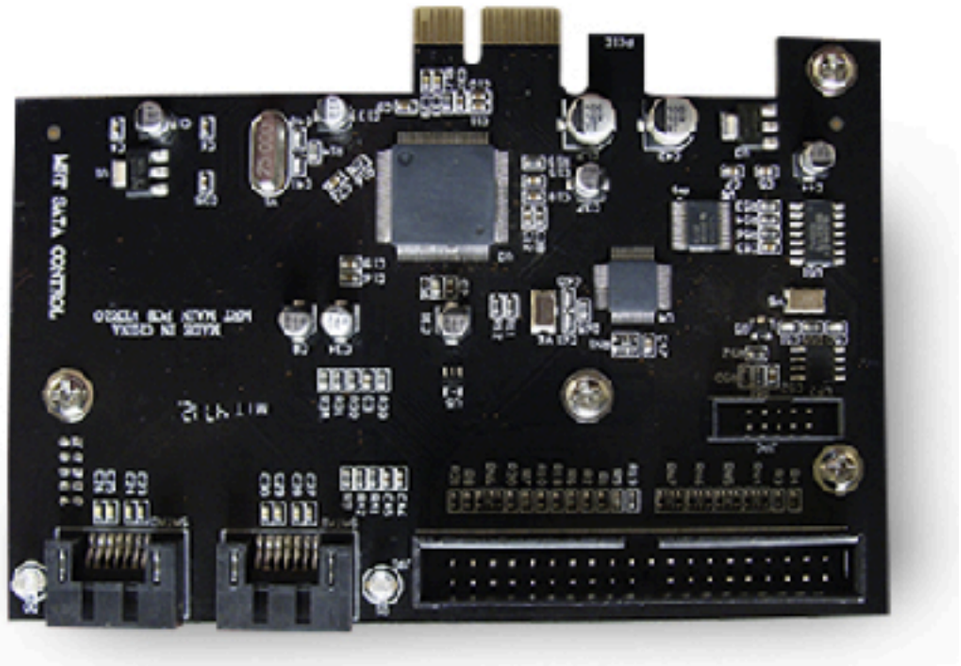
OSSLab

SATA 邏輯分析儀



OSSLab

資安硬體界的黑吃黑



OSSLab

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

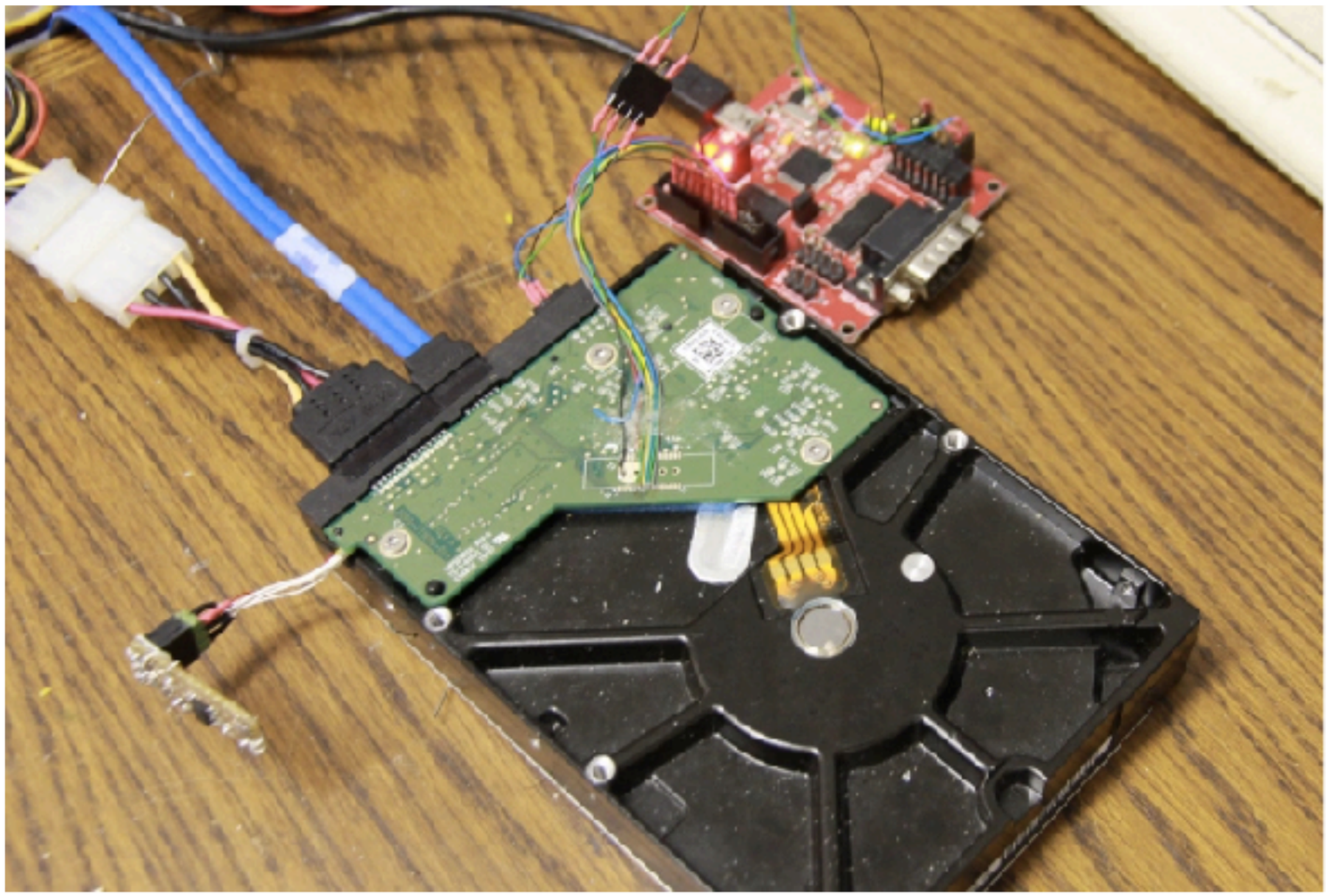
韌體裡面通常有一個命令解析引擎

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

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

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

OSSLab

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

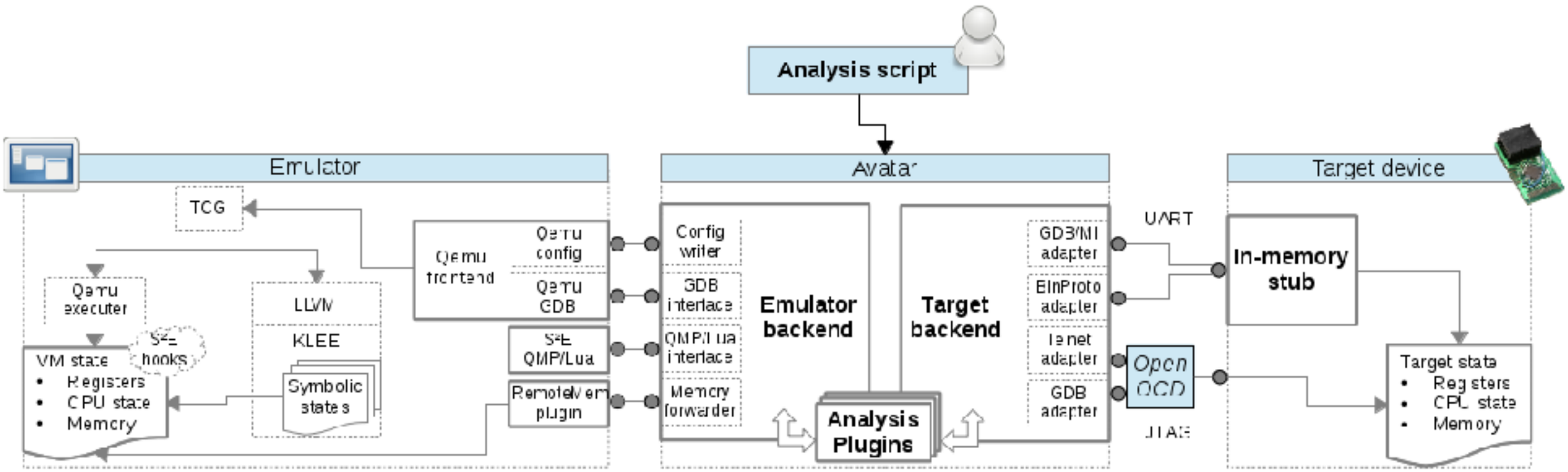
```
Tech Unlock Handshake: 0x1CEF53D8
Reply:
```

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


Analysis script
Emulator
Avatar
Target device
TCG
Qemu executer
LLVM
KLEE
VM state
Registers
CPU state
Memory
S2E hooks
Symbolic states
Qemu frontend
Qemu config
Qemu GDB
S2E QMP/Lua
RemoteMem plugin
Config writer
GDB interface
QMP/Lua interface
Memory forwarder
Emulator backend
Target backend
Analysis Plugins
GDB/MI adapter
ElfProto adapter
Telnet adapter
GDB adapter
UART
OpenOCD
JTAG
In-memory stub
Target state
Registers
CPU state
Memory

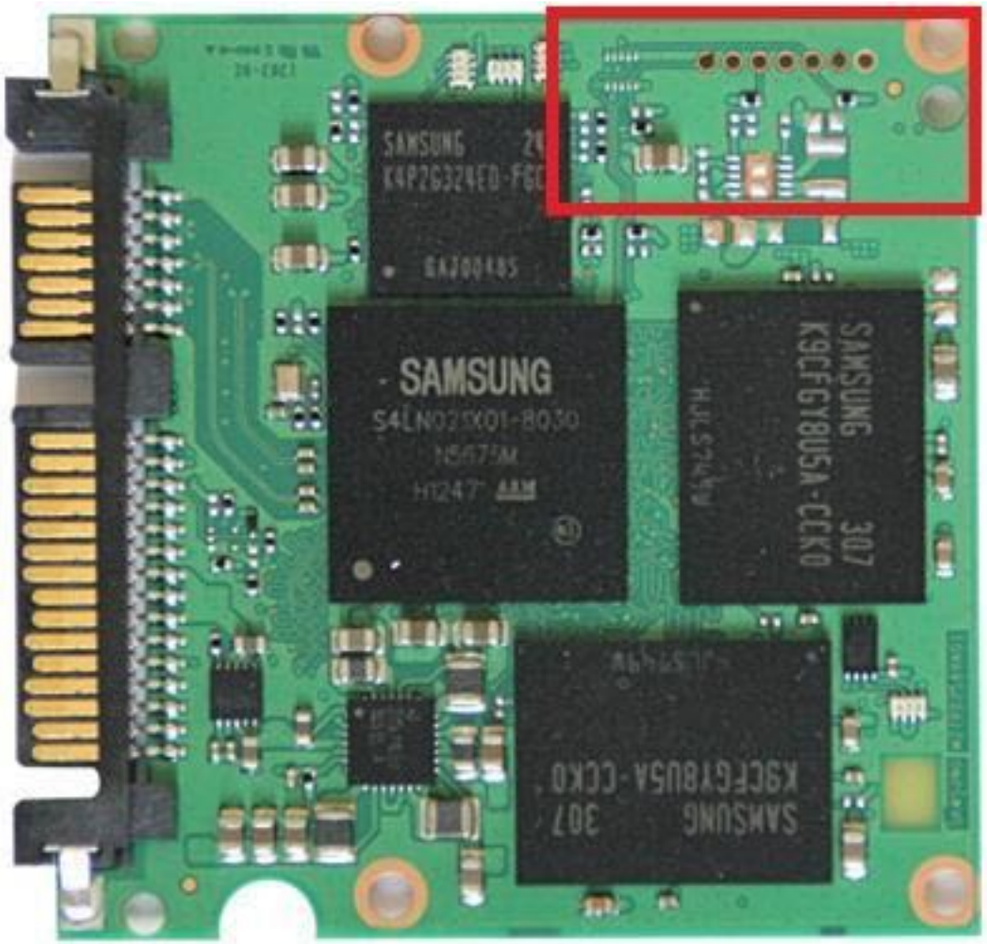
OSSLab

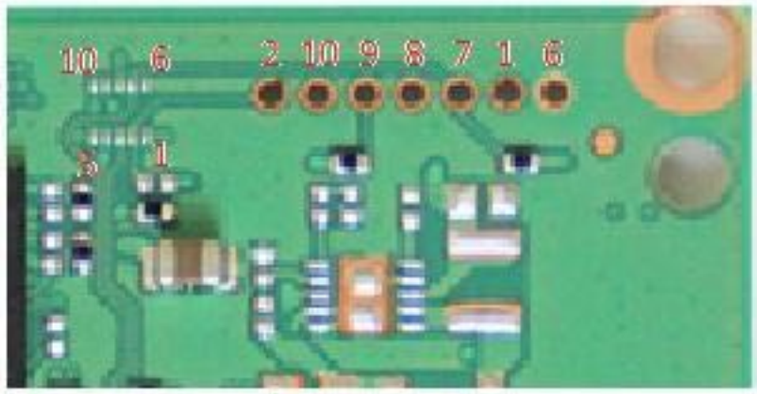
結束

應用與原理必須相結合

Q&A

OSSLab

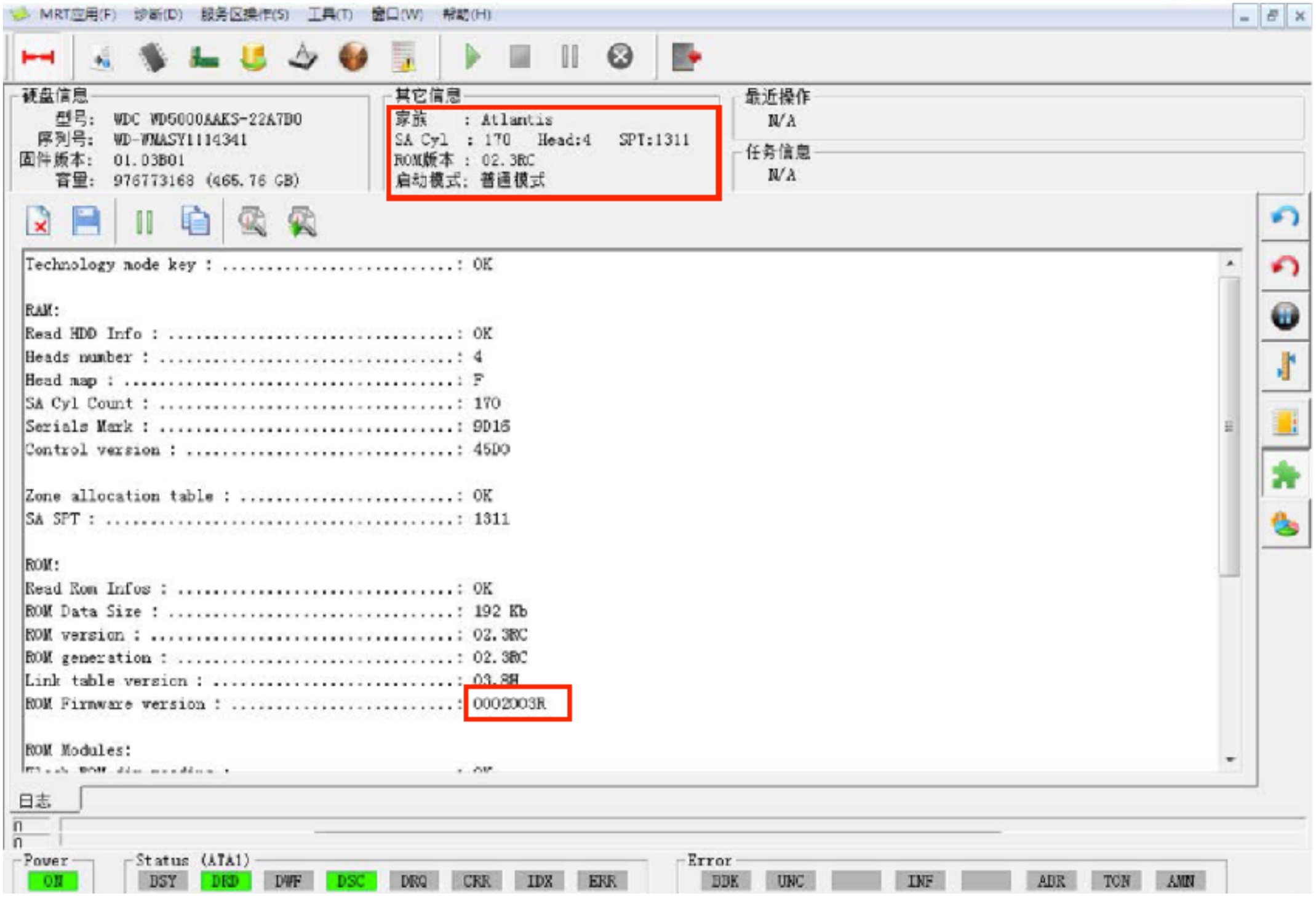

SAMSUNG
K4P2G324ED-FG
SAMSUNG
S4LN025X01-B030
SAMSUNG
K9CFGY8U5A-CCK0
307


10 6
2 10 9 8 7 1 6
5 1

OSSLab

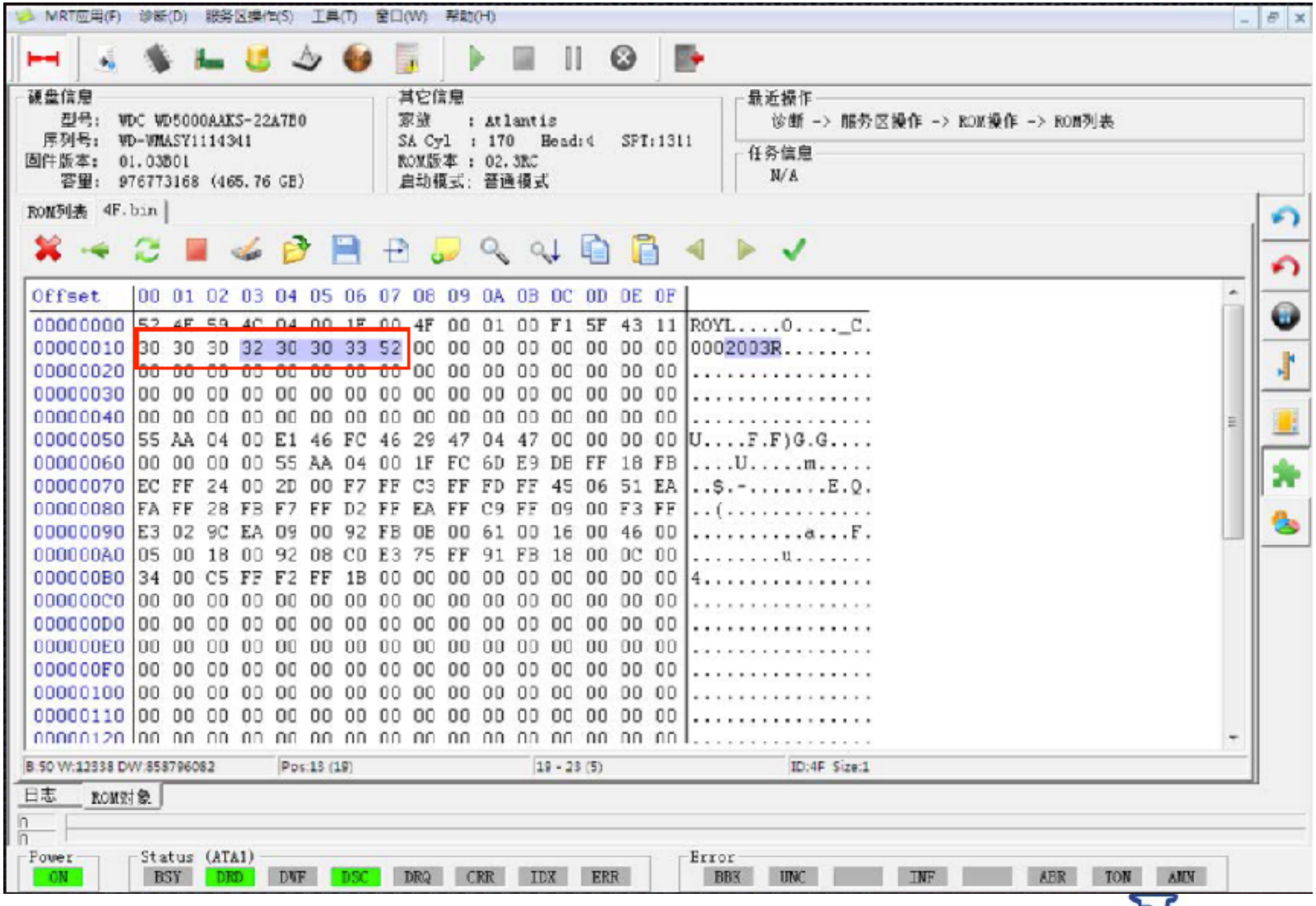
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000000	25	B0	EE	8A	EE	EF	A6	22	18	2B	8D	32	15	98	E2	E2
00000000010	C3	B3	6D	C5	BD	FF	20	FA	E9	43	7E	AE	0E	69	0C	ED
00000000020	CB	84	FB	90	7F	D4	F8	91	AE	CA	37	B9	33	8F	47	61
00000000030	E3	12	82	58	4B	CD	34	6E	12	12	F8	47	D9	5F	29	49
00000000040	8F	26	2C	E3	8B	5D	88	FC	7D	E4	92	18	C3	59	CD	2F
00000000050	44	32	9A	A6	DF	98	D7	ED	A2	27	39	D7	6E	1D	C7	D5
00000000060	6D	90	27	67	7C	F2	F0	84	23	54	C2	13	82	01	BA	15
00000000070	51	34	C1	72	54	5B	55	B8	82	C4	A7	64	1A	35	F8	5E
00000000080	81	7F	4E	4A	9E	F1	FB	70	A3	1D	17	58	1C	3D	7B	3C
00000000090	50	7B	5E	71	37	94	D3	A6	D7	1C	1C	4D	8A	9D	FB	BE
000000000A0	2B	8E	16	7F	15	38	14	2E	0E	ED	0C	55	30	9C	99	38
000000000B0	38	23	CD	48	6A	5D	9D	53	F7	3B	25	2B	2E	25	62	F6
000000000C0	E1	E4	76	07	3D	59	CB	64	38	94	C4	4B	9D	8A	34	B6
000000000D0	6B	FE	D9	EC	FF	20	70	10	46	14	F8	C2	D5	EA	EC	4E
000000000E0	56	71	43	66	88	EE	7A	12	73	A8	82	8B	2F	9B	CB	20
000000000F0	C9	A9	3E	D6	A8	5A	93	5B	20	C1	7C	14	E2	F3	4B	B8
00000000100	C2	58	C6	EE	99	10	EA	D2	A9	B3	2E	5C	27	C5	5E	B0
00000000110	D0	F3	1E	14	93	27	D5	CB	AE	D9	F6	2E	B1	0B	8B	49
00000000120	64	6C	3A	43	9B	FB	03	05	14	A6	4B	7F	B6	B0	5A	09
00000000130	1F	74	59	EF	B7	EE	7C	19	AE	57	FA	FB	04	F4	21	EF
00000000140	28	9E	23	BE	2E	88	EE	7B	63	36	B5	61	1E	3C	4E	13
00000000150	75	B5	59	73	74	F6	44	00	C8	DC	99	4E	22	C5	F7	65
00000000160	7A	AD	CC	B1	94	12	06	F6	B1	35	57	20	E0	AD	00	D9
00000000170	4B	49	03	42	28	C2	94	F0	B2	3F	BA	E1	46	3E	86	DF
00000000180	F2	A9	C9	0F	03	E9	0D	7C	01	C2	E2	65	49	1A	17	48
00000000190	D5	80	9A	D7	75	EF	64	E6	4B	15	02	FD	31	F8	6D	60
000000001A0	92	94	BD	8B	30	49	94	CE	0A	2E	8B	81	06	1F	EE	56
000000001B0	AB	6C	42	49	A8	64	36	C4	31	FC	BC	70	97	C9	D9	82
000000001C0	27	91	8E	89	77	4F	E6	27	C8	AC	58	05	EC	7E	7E	F0
000000001D0	06	6E	37	93	F7	9D	7C	1C	09	4C	73	F1	AD	4A	A9	B4
000000001E0	94	95	CB	A0	0D	30	75	BE	94	18	3E	AA	3B	8C	70	77
000000001F0	8D	1F	33	55	83	9D	24	9C	3E	F8	D6	4B	FF	41	89	B8

WD 硬碟重要參數



OSSLab

ROM微代碼版本號



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

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

OSSLab