

行政院所屬各機關因公出國人員出國報告書
(出國類別：實習)

參加「毀損硬碟資料回復訓練課程」心得報告

服務機關：法務部調查局
出國人姓名：鄭健行調查官，劉秉昕調查官
出國地點：香港
出國期間：中華民國 101 年 10 月 29 日至 11 月 2 日
報告日期：中華民國 101 年 12 月 28 日

報告大綱

壹、 行程記述.....	3
貳、 訓練公司簡介.....	3
參、 訓練課程記要.....	4
肆、 心得與建議.....	33
附錄：附表及訓練照片.....	35

壹、行程記述

此次行程主要是參加美國 Ji2 公司在香港順安達科技有限公司（DataExpert Technology Limited）場地舉辦之「毀損硬碟資料回復」教育訓練，期程為 10 年 10 月 29 日至 11 月 1 日，共計 4 日，課程內容著重於診斷毀損硬碟損壞狀況及回復資料之實作方法，第一日主要講述資料復原實驗室的標準作業程序及資料復原設備簡介，第二日則是講解硬碟架構、故障剖析以及基礎的復原流程，第三日實際練習 P C B 板的修復及無塵室的使用，第四日介紹硬碟修復工具 (Atola)。課程內容有四大目標：一、瞭解硬碟內的各項元件以及各元件之間運作的原理。二、如何使用目前資料復原的軟體及工具去診斷硬碟故障的原因。三、根據診斷的結果制定不同的修復策略。四、介紹各種硬碟常見的故障情況及修復程序進而去完成修復。

貳、訓練公司簡介

Ji2 公司是 2001 年在美國南加州成立，目前在美國、東京、香港、台灣均有設置分公司及據點，其主要服務的項目是提供 eDiscovery-數位驗證及 Digital Forensics-數位鑑識，該公司在 eDiscovery 部分是指在訴訟的程序中對於數位證據提供司法鑑定上的諮詢顧問及技術指導並發現己方之有力證據，而 Digital Forensics 則是對於數位證物給予更深入的科技檢驗，以科學的方法找出有力證據。而 Digital Forensics 的第一步就是 Data recovery，對於現今最常使用的儲存裝置-「硬碟」，予以修復及取證，所以該公司不僅投入在硬碟修復領域，另外也研發有關硬碟修復、儲存、資料抹除及破壞等相關鑑識產品，包括有硬碟複製機、參加「毀損硬碟資料回復訓練課程」心得報告----- 3 -/39

硬碟消磁機、硬碟破壞器等，相關設備如下圖所示。



圖 2.1 硬碟消磁機、硬碟破壞器



圖 2.2 硬碟修復區

參、訓練課程紀要

一、第一日，10月29日於上午到達後，至上課地點香港順安達科技有限公司參訪，由該公司顧問兼本次上課講師范先生接待，簡單介紹該公司的服務項目後，對於資料復原標準程序，資料復原的四個階段以及對於硬碟無法修復的狀況做說明，內容如下：

(一)資料復原的四個階段

- 1.Diagnosis：診斷檢查並確認硬碟受到損傷部分，檢查的部分包括 PCB 板、硬碟驅動器、韌體、馬達或硬體零件等。
- 2.Recovery：針對損傷部分使用設備進行恢復，或者進行零件更換，對於硬體損傷的部分通常以經驗來判斷及解決這些損傷的問題
- 3.Imaging：硬碟修復後必須開始進行複製或恢復內容，因為修復後的硬碟未必能 100%的將資料讀出，因此可利用一些硬體設備或是軟體工具對硬碟做 image(映象檔)複製，儘快將修復好的硬碟把資料備份出來。
- 4.File restoration：此一部份是指對邏輯性文件進行復原工作，對於已刪除的資料或檔案名稱已遭覆蓋的資料進行還原，通常一般的商用工具軟體可做到這些功能。

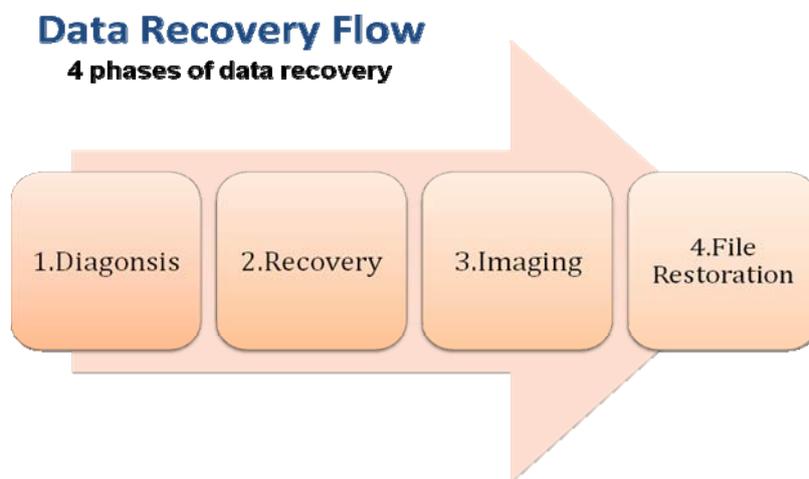


圖 3.1.1 Data Recovery Flow

(二)資料無法復原的情況：

損傷硬碟資料無法達到 100%的復原狀況，而商業化的資料復原一般都在無塵室（cleanroom）內進行，包括磁頭更換，主軸馬達及線路更換，或是 PCB 電

參加「毀損硬碟資料回復訓練課程」心得報告----- 5 -/39

路板維修以及韌體（firmware）數據維修等，雖然很多廠商號稱可以達到修復率99%以上，但目前都沒有數據證明，對於硬碟修復而言，以下有幾種情況硬碟資料將可能無法復原。

1. Part-replacement（零件更換），根據統計顯示，只要硬碟有更換零件的動作，一般資料成功復原的機率大約剩下40%~60%之間。
2. 有些廠牌硬碟修復的成功率較高，有些廠牌修復率則接近於零，因此要視硬碟廠牌及使用的驅動模組（drive model）而定。
3. 如果是物理性的破壞如水淹、火災、撞擊等，也將無法復原，如下圖所示。



圖 3.1.2 物理性破壞

4. 在PCB(printed circuit board)板上的(burnchip)損壞，也將無法復原，因為 burnchip 內含硬碟出廠時的一些重要參數值，硬碟啟動時必須讀取此參數才能運作，如下圖所示。

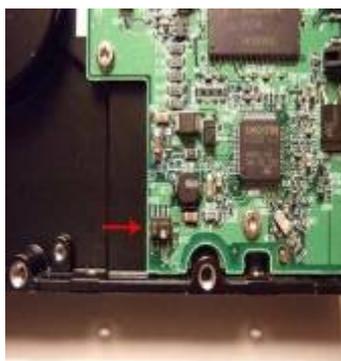


圖 3.1.3 burnchip 損壞

5. 硬碟韌體（firmware）內某些重要模組損壞也將無法恢復。
6. 硬碟碟盤有刮傷、刮盤的情形時，也將無法復原，如下圖所示。



圖 3.1.4 硬碟磁盤刮盤

二、**第二日**，10月30日，本日主要是對於硬碟構造及 PCB 板的維修重點進行講解，而硬碟的維修部分大多要仰賴 donor（另一顆同廠牌型號硬碟）來進行零件替換，當一個故障的硬碟有一個 donor 可進行零件替換時，那資料成功復原的機會就會提升不少。

(一)硬碟構造簡介：要維修硬碟前最重要的是瞭解硬碟的構造，一顆硬碟如下圖

總共可分為下列各項元件：

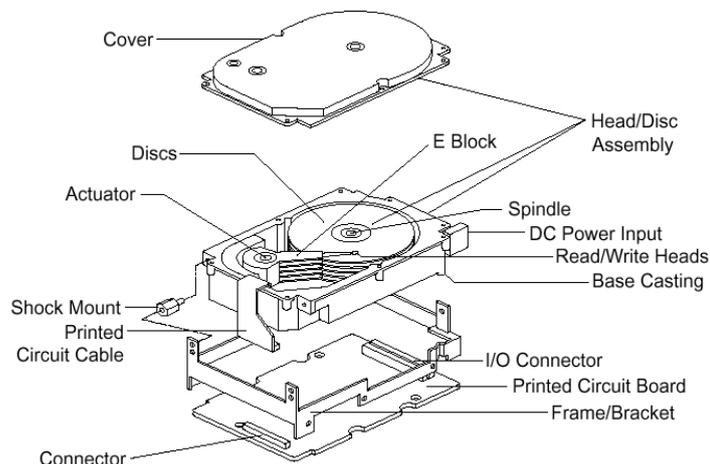


圖 3.2.1 硬碟構造

1.Cover(上蓋)	9.Spindle(軸承)
2.Discs(磁盤)	10.DC Power Input(直流電源輸入)
3.Actuator(驅動臂)	11.Read/Write Heads(讀/寫頭)
4.Shock Mount(防震架)	12.Base Casting(底殼)
5.Printed Circuit Cable(電路板連接線)	13.I/O connector(I/O 連接器)
6.Connector(連接器)	14.Printed Circuit Board(印刷電路板)
7.Head/Disc Assembly(磁頭及碟片裝置)	15.Frame/Bracket(外框/支架)
8.E Block(磁臂組)	

(二)硬碟印刷電路版各項元件簡介：

Printed circuit board (PCB) 印刷電路板元件介紹：

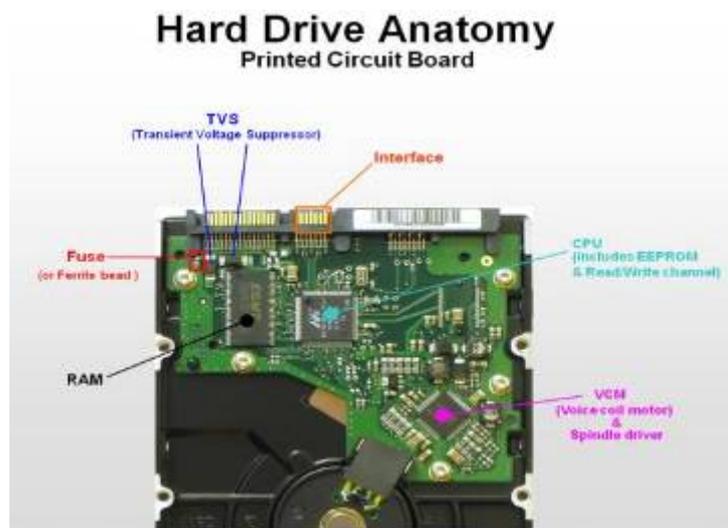


圖 3.2.2 印刷電路板(PCB)元件

1. Voice coil motor & Spindle driver(VCM):

馬達及軸承控制晶片：由 CPU 傳遞信號控制，在不同的電流作用下，可以很精確的控制馬達加速度和負加速度，讓碟盤在啓動及停止時正常的運轉；軸承則負責帶動磁頭的徑向轉動，使磁頭得以任意更換磁軌，並使磁頭的末端產生磁場作用，藉而讀取/寫入資料。



圖 3.2.3 PCB 板上各類 VCM

2. Transient Voltage Suppressor (TVS) :

瞬態電壓抑制器：TVS 是一種限制電壓型的過壓保護器，它將瞬間過高的電壓鉗制至一個安全範圍，藉以保護後面的電路，它有著比其它保護元件更快的反應時間，因此常用於可攜式設備如筆記型電腦、手機、PDA、MP3 播放器等電路內，在硬碟的印刷電路板上通常該元件會有白色的一條線，用以分辨正負極性。



圖 3.2.4 PCB 板上各類 TVS

3. Fuse or ferrite bead

保險絲或鐵氧體磁珠：保險絲最主要的功用就是防止超量的電流流過電子電路。超額的電流流過保險絲時將使它產生高溫而導致熔斷，以保護電路免於受到傷害，可以說保險絲是電器設備的一個安全開關，因此以三用電表量測時

應該為通路的状态，當保險絲損毀時以三用電表量測則呈現斷路的状态，有時在 PCB 板上會標示 F 的字樣代表保險絲。

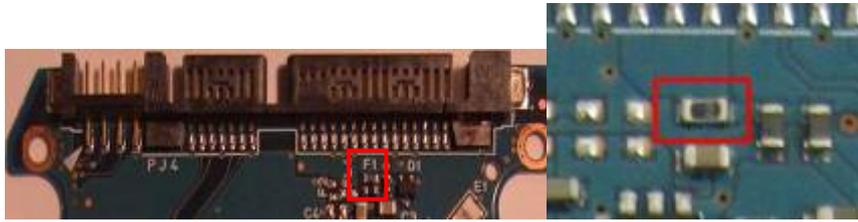


圖 3.2.5 PCB 板上的 Fuse

4.CPU(May include EEPROM or NVRAM , R/W channel)

中央處理器：在 PCB 板上用來控制，接收輸入指令後來控制 R/W channel 及 Voice coil motor，有些 PCB 板上的 CPU 還會搭配 EEPROM or NVRAM 或 R/W channel，或是直接把 EEPROM or NVRAM 或 R/W channel 製作於 CPU 內。



圖 3.2.6 PCB 板上的 CPU

(三)如何尋找 donor 硬碟？

當硬碟損壞需要更換零件時，就必須尋找一顆 donor 硬碟，把該正常硬碟上的元件拿來更換，而如何尋找一顆 donor 硬碟呢？就必須瞭解硬碟背蓋上的資訊，儘量找到資訊相符合的 donor 硬碟來進行替換。

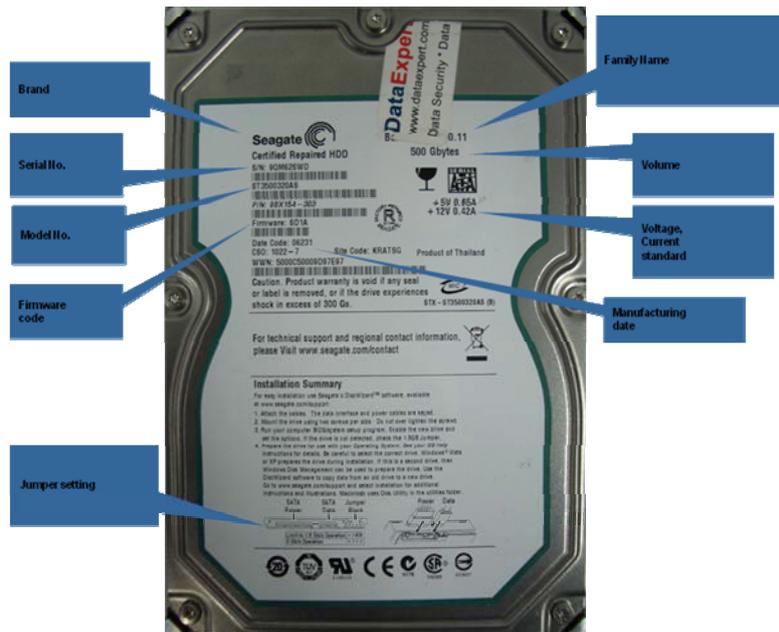


圖 3.2.7 donor 硬碟資訊

而硬碟上的資訊包括有：

- 1.Brand(廠牌)
- 2.Serial No.(序號)
- 3.Model No.(模組序號)
- 4.Firmware code(韌體編號)
- 5.Jumper setting(跳線設定)
- 6.Family Name(家族名稱)
- 7.Volume and interface (容量和介面)
8. Voltage, Current standard(電流及電壓標準值)
9. Manufacturing date(製造日期)
10. Product of country(生產國家)

其中最好 Model No.(模組序號)、Firmware code(韌體編號)、Family Name(家族名

稱) 、Product of country(生產國家)能與原硬碟相符最好。

(四)硬碟 PCB 板 Troubleshooting 流程：

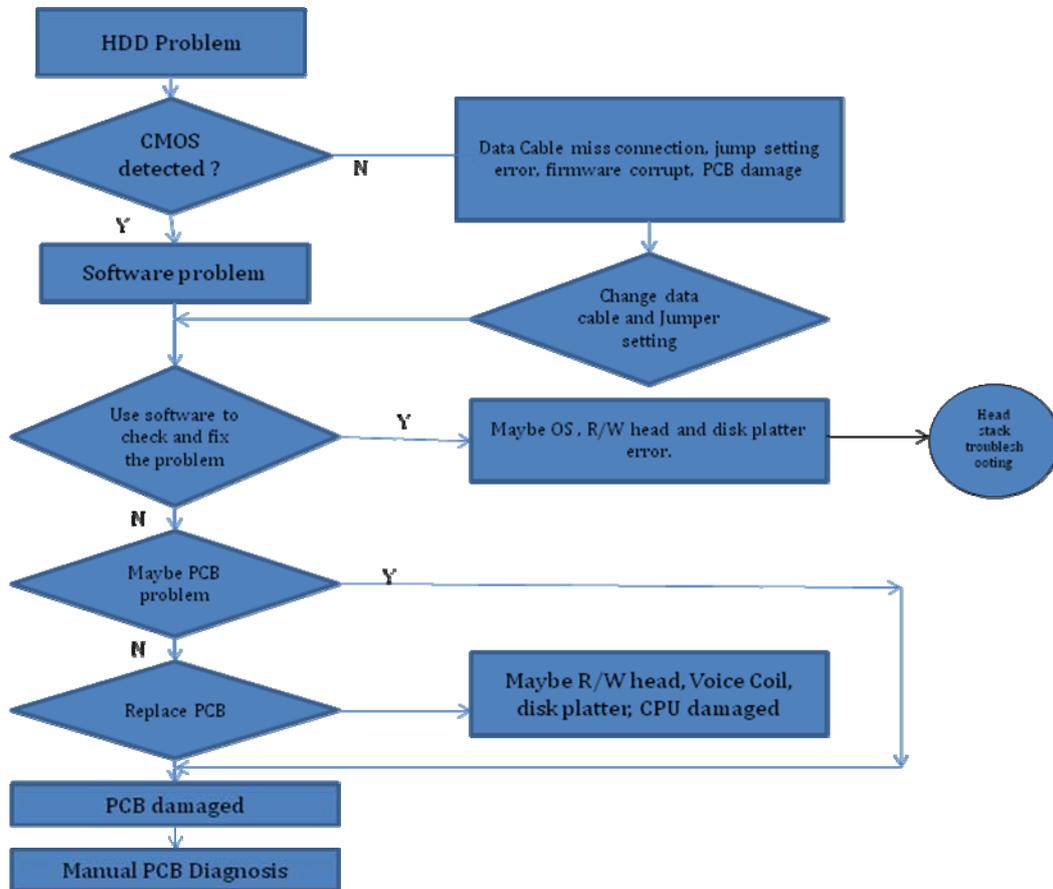


圖 3.2.8 硬碟 PCB 板 Troubleshooting 流程

三、**第三日**，10 月 31 日，本日主要以實作 PCB 板維修及硬碟內部零件更換為主，從實作當中去瞭解如何檢測故障的部分，並可透過實作加強印象，瞭解硬碟各部分零件構成的原理。

(一)PCB 板維修實作：一般而言，若是 PCB 板故障，就必須要找一個 donor，將 donor 上正常的 PCB 板零件與故障的 PCB 板做交換，而在交換之前最好先以三用電表檢測 PCB 板上的輸入電壓及各項元件是否正常，檢測內容包括電源電壓、TVS 電壓、Fuse 電壓、線圈電阻及電路板線圈輸出電壓是否正

常，測量後判斷故障的 PCB 板上那個元件有問題，再把正常的 PCB 板上正常元件如 TVS、EEPROM 或 Burn chip 及 VCM 以取下後與故障的 PCB 版零件進行更換，再重新檢測。

(二)檢測方式如下：

1. 三用電表檢查輸入電源是否正常，如下圖所示。

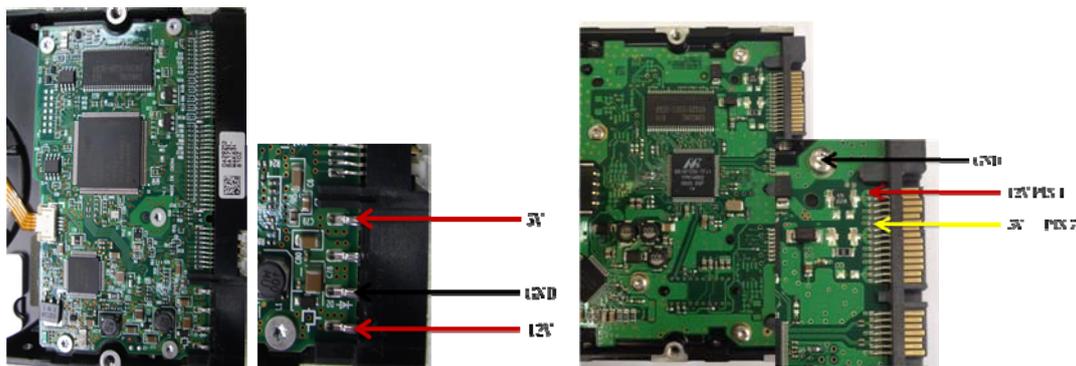


圖 3.3.1 檢查輸入電源

2. 使用三用電表檢查 TVS 電壓是否正常，如下圖所示。



圖 3.3.2 檢查 TVS 電壓是否正常

3. 接上電源後使用三用電表檢查馬達電源是否正常，如下圖所示。



圖 3.3.3 檢查馬達電源

4. 將三用電表撥至電阻 Ω ，檢查馬達線圈電阻是否正常，如下圖所示。



圖 3.3.4 檢測線圈歐母值是否一致

(三)PCB 板維修工具：工欲善其事，必先利其器，在進行 PCB 板的維修前需要準備一些手工具用來進行 IC 零件的拆取及銲回，工具包括以下所示，其中 99%濃度之酒精主要是用來清潔銲過後的 PCB 板，另外當拆取或更換硬碟磁盤及磁頭時，若是有指紋或灰塵沾染到磁盤上時，亦可用棉花棒加上酒精進行清潔，有時若磁頭讀取不順時亦可用酒精清潔。

1.熱風槍



圖 3.3.5 熱風槍

2.可溫控式烙鐵



圖 3.3.6 可溫控式烙鐵

3.各式手工具（起子、夾子）



圖 3.3.7 各式手工具

4.三用電表

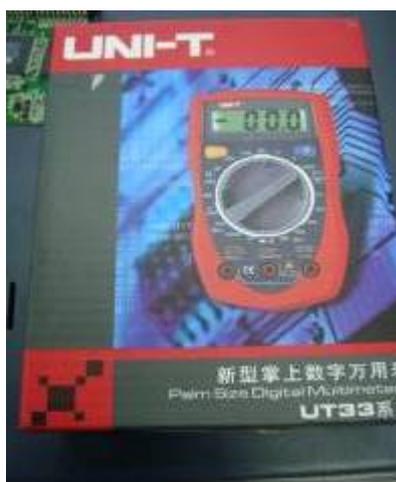


圖 3.3.8 三用電表

5.99%濃度酒精



圖 3.3.9 酒精

6.放大鏡



圖 3.3.10 放大鏡

7.工作平台



圖 3.3.11 工作平台

(四)實作項目一：量測 PCB 板上各元件電壓，確認電壓是否正常後，將 PCB 板 TVS 以熱風槍拔下後再焊回，將 PCB 板裝回硬碟後看是否可以正常起動。

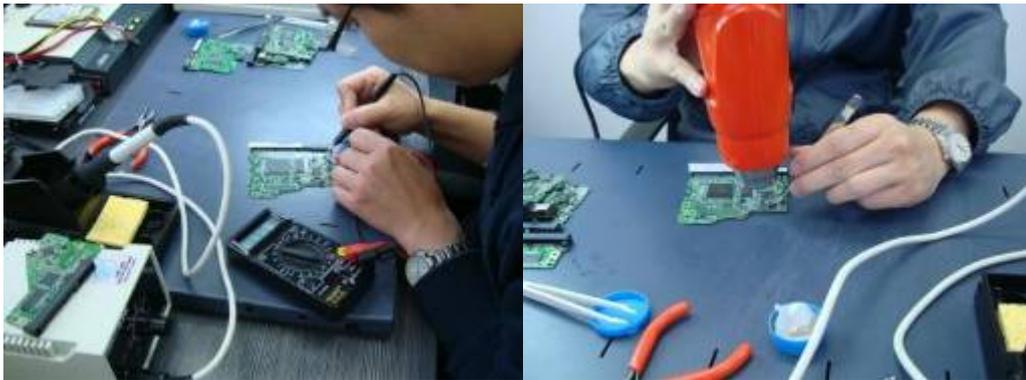


圖 3.3.12 量測各元件電壓

使用熱風槍將 TVS 取下



圖 3.3.13 再將 TVS 鉗回

(五)實作項目二：將 PCB 板上的 EEPROM 以熱風槍取下後，再用烙鐵焊接回去，將 PCB 板裝回硬碟後看是否可以正常起動。



圖 3.3.14 使用熱風槍取下 EEPROM 後再焊回去

(六)實作項目三：將 PCB 板上的 VCM CHIP 以熱風槍取下後，再用烙鐵焊接回去，將 PCB 板裝回硬碟後測試是否可以正常啓動。

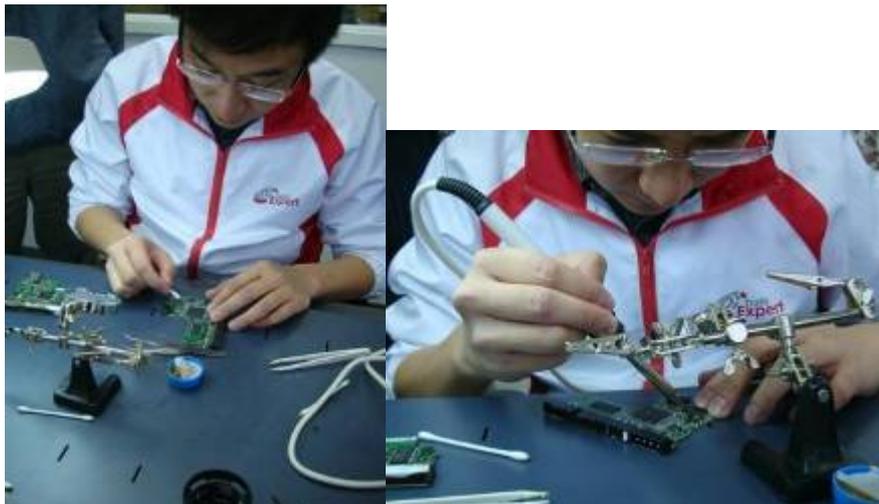


圖 3.3.15 使用熱風槍取下 VCM CHIP 後在鉚回去

(七)硬碟驅動元件介紹：硬碟內部的元件稱為 Head-disk assembly 或簡稱(HDA)，硬碟記錄的方式是使用磁碟盤片及磁頭。利用磁化的盤片存儲數據，並使用磁頭改變這些磁場去讀取或寫入。磁頭的部分也有很多組件，稱為 Head Stack Assembly 或簡稱(HAS)，硬碟內部構造如下：

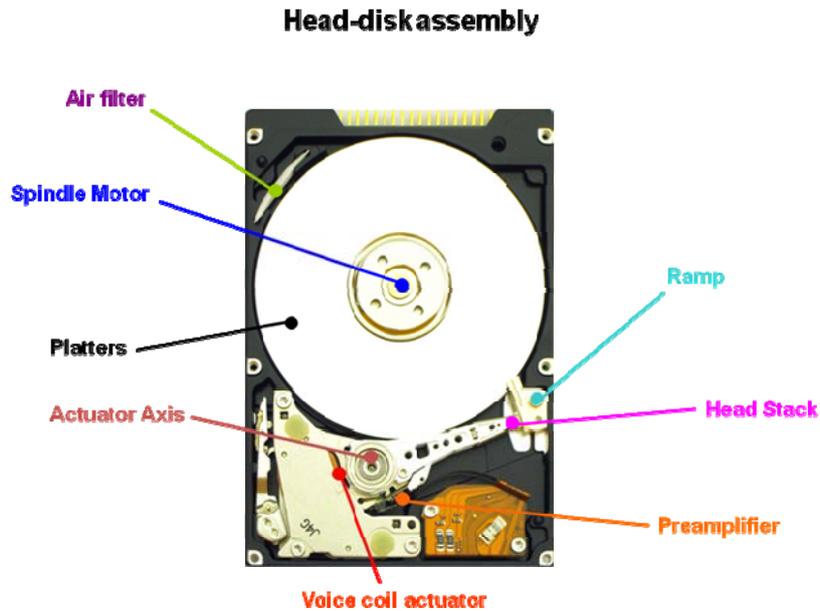


圖 3.3.16 硬碟內部構造

1. Air filter(空氣過濾器)
2. Spindle Motor(主軸馬達)
3. Platters(磁碟盤片)
4. Actuator Axis(驅動手臂)
5. Voice coil actuator(音圈馬達)
6. Ramp(磁頭停放區)
7. Head Stack(磁頭)
8. Preamplifier(前級訊號放大器)

硬碟內部 Drive Errors 的狀況：

1. 硬碟磁頭故障導致無法讀取。
2. 錯誤檢查及校正訊息顯示所的 block 都無法讀取的狀態。
3. 有時停電造成磁頭卡住的問題。

4. 碟盤壞軌過多以致於磁頭不斷停留讀取同一區塊。
5. 主軸馬達發生故障導致旋轉不順。

在開盤維修前必須注意的事項：

1. 馬達是否有轉動？
2. 是否有敲盤的聲音？
3. 通上電源時是否有啓動及磁盤旋轉的聲音，停止時是否有降速的聲音。
4. 是否有過熱的情況。
5. 看一下 PCB 板是否有燒焦的痕跡，或是過熱的現象。
6. 看一下有關的文件及拍照記錄狀況。

開盤後需要注意的事項：

1. 看一下磁頭是否停留在磁盤的正確位置。
2. 看一下空氣過濾器或磁盤是否有卡灰塵。
3. 看一下磁頭是否有損壞。
4. 看一下是否有刮盤的情況。
5. 看一下主軸馬達是否有問題。

(八)硬碟驅動元件 Troubleshooting 流程

Proper Head Stack Diagnosis

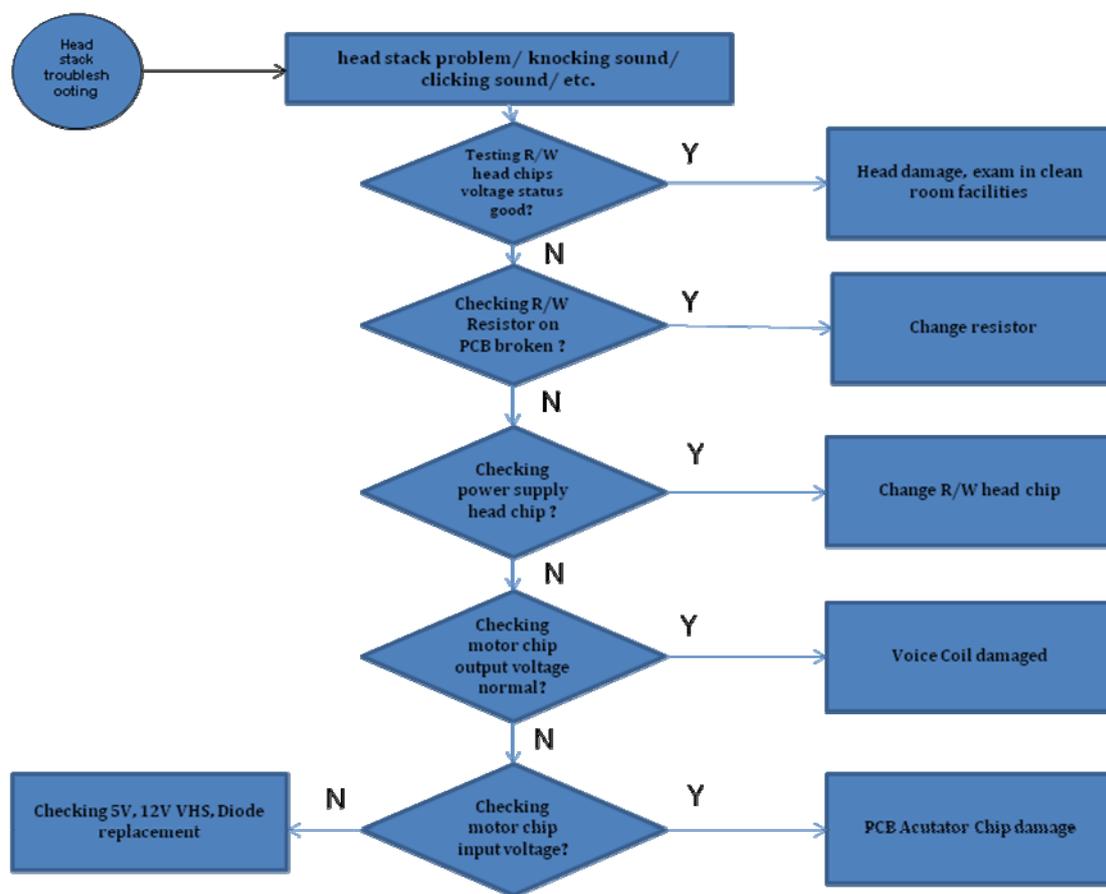


圖 3.3.17 硬碟驅動元件 Troubleshooting 流程

(九)磁頭更換實作：本實作係假設硬碟磁頭故障利用 donor 進行磁頭更換，開盤後將磁頭取出，再將磁頭安裝回去，安裝完畢之後以 Atola 進行硬碟檢測。



圖 3.3.18 磁頭更換實作

(十)磁盤更換實作：本實作係假設硬碟的線圈馬達發生故障，係將故障的硬碟磁參加「毀損硬碟資料回復訓練課程」心得報告----- 21 -/39

盤更換到 donor 上，本實作是把磁盤取出後再安裝回去，安裝完畢之後以設備（Atola）進行硬碟檢測。一般而言更換磁盤成功率會更低，因為硬碟的磁盤只要有 2 個以上，取出時磁盤垂直的磁柱若稍微有點偏移，安裝回去之後就會讀取不到，除非必要，則是儘量不更換磁盤。更換情形如下圖所示。

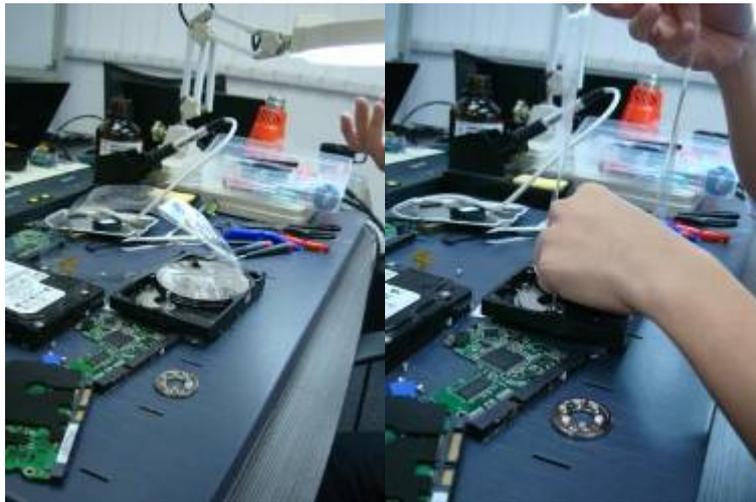


圖 3.3.19 磁盤更換實作

四、第四日，11 月 1 日，本日主要係介紹 Atola 硬碟檢測及修復工具操作，Atola 是一個硬體式的商業化硬碟檢測工具，它可以用來檢測硬碟各元件的狀況，並產生檢測報告，可提供維修人員快速的判斷硬碟損傷的部分，它也可以自動的修復某些廠牌硬碟的韌體，以及某些硬碟 ATA 密碼加解密及設定，並且可設定讀取的規則，當硬碟有壞軌時可跳過壞軌的區域儘量把硬碟的資料讀取出來。



圖 3.4.1 Atola 硬碟檢測工具

(一)硬碟檢測(Diagnostic Functions):Atola係使用網路線配合電腦軟體去控制及操作，該軟體如圖3.4.2所示，要檢測硬碟只要把它接上Atola的主機後，選擇好介面種類，按下軟體左側Automatic Checkup，就會開始進行檢測，當檢測完畢後就會產生一個檢測報告，告訴你硬碟目前的狀況，若有損害的地方就會出現損壞狀況的訊息，告訴你硬碟那個部分發生了問題，維修人員可以依據報告的內容做為參考進行維修。

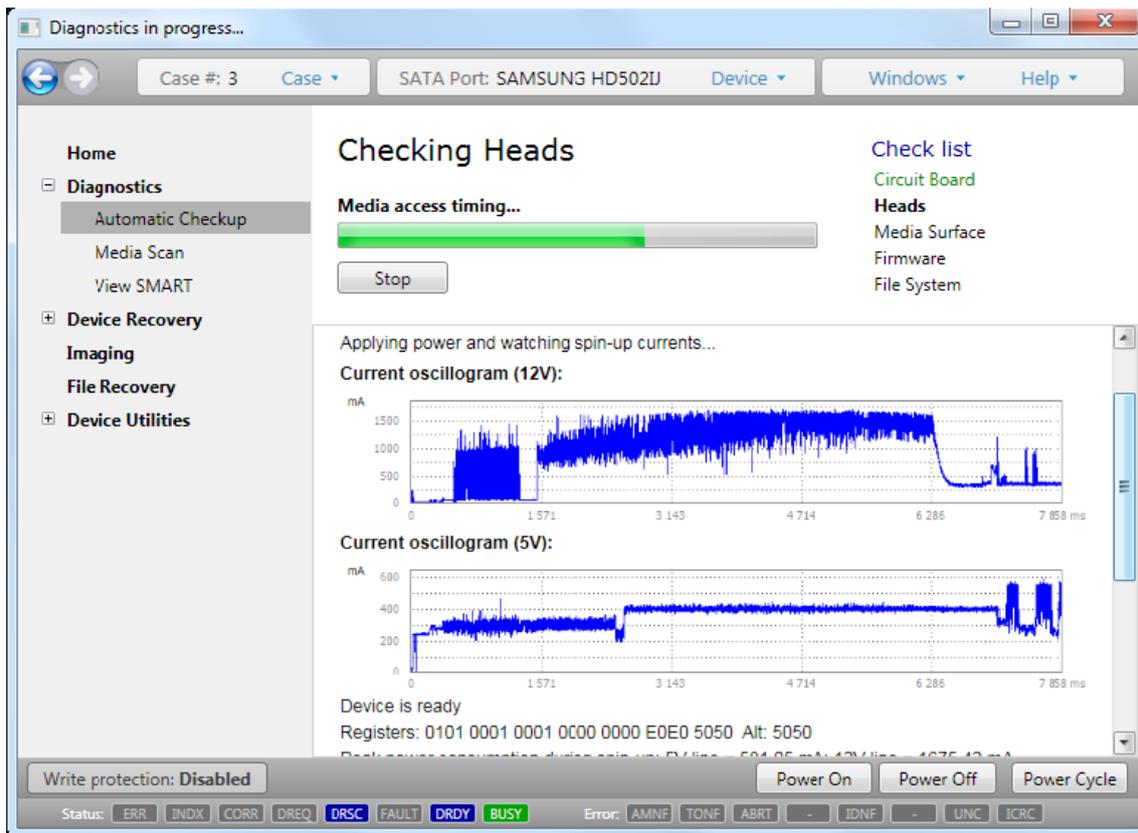


圖 3.4.2 Atola 軟體操作畫面

(二)Atola Diagnostic Report：檢測報告包括五個項目，PCB Checkup(PCB電路板的檢查)、Head Checkup (硬碟磁頭的檢查)、Media scan (媒體介面掃描)、Firmware Area (System Area) Checkup (韌體的檢查)、Partitions and File Systems Checkup (分割區及檔案系統檢查)，且會依照順序檢查，每當檢查完一項就會在後面告訴你檢查的結果，以下是一個正常硬碟檢測報告的樣本，如下所示。

Automatic Checkup finished

Report date and time: 2012/11/21 at 上午 10:26

Atola Insight v2.5.4423.31284

DiskSense unit: Ethernet

Device information:

ST3500418AS

Serial number: 9VM4RSX0

Firmware revision: CC44

Capacity: 976,773,168 sectors or 500,107,862,016 bytes

512 bytes per sector

Diagnostics results

No major hardware or firmware issues have been found.

Full Diagnostic Log

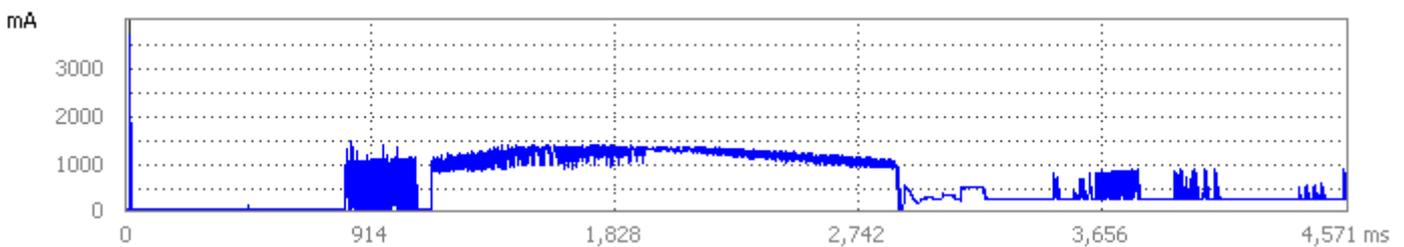
Circuit Board (PCB)

Selected Interface: SATA

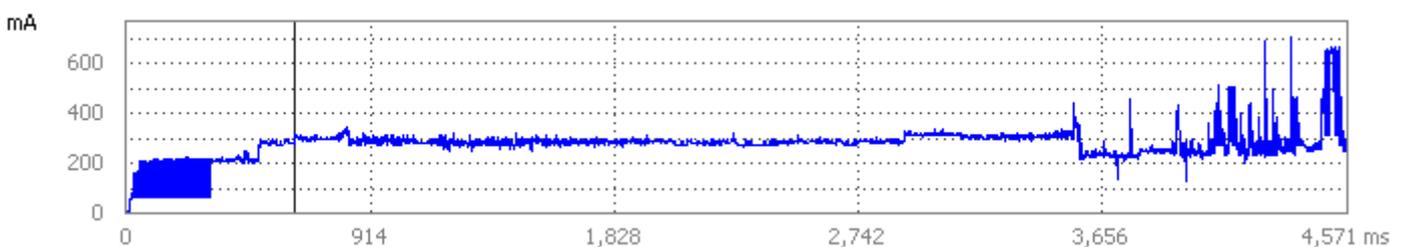
Device is powered on. A power cycle is needed...

Applying power and watching spin-up currents...

Current oscillogram (12V):



Current oscillogram (5V):



Device is ready

Registers: 0101 0001 0001 0000 0000 E0E0 5050 Alt: 5050

Peak power consumption during spin-up: 5V line = 689.70 mA; 12V line = 3621.42 mA

Status register seems to be valid.

Interface check passed.

Device has been identified: ST3500418AS SN: 9VM4RSX0

Elapsed: 22 sec.

Circuit board looks fine

Heads

Checking power consumption curves for signs of head damage

Identifying the device

Detecting device family

All device identification checks have passed.

Detected 2 heads: 0 1Performing media access timing verification separately for each head.

Head 0:

Verified sectors: 276,214

Errors: 0

Avg. speed: 88 MB/s

Status: OK

Head 1:

Verified sectors: 374,963

Errors: 0

Avg. speed: 78 MB/s

Status: OK

Media access timing verification shows no damage to the head stack.

Elapsed: 8.6 sec.

Head stack looks fine

Media Surface

Media scan is running...

Verifying outer tracks (LBA: 0 - 600,064)

0 error(s) found

Verifying middle tracks (LBA: 488,386,583 - 488,986,647)

0 error(s) found

Verifying inner tracks (LBA: 976,173,103 - 976,773,167)

0 error(s) found

Elapsed: 9.7 sec.

Media surface looks fine

Firmware

Device is not locked.

Device identification data looks fine.

Max Address according to device ID: 976,773,167

Native Max Address Ext: 976,773,167

Max Address from DCO: 976,773,167

Reported capacity looks logically correct.

Performing SMART checks...

#	Attribute Name	Value	Worst	Threshold	RAW
1	Read error rate	117	99	6	144,611,561
3	Spin up time	97	97	0	0
4	Number of spin-up times	100	100	20	821
5	Reallocated sectors count	100	100	36	0
7	Seek error rate	81	60	30	121,443,387
9	Power-on time	93	93	0	6,920
10	Spin-up retries	100	100	97	0
12	Power Cycles	100	100	20	821
183		100	100	0	0
184	End to End Error	100	100	99	0
187	Reported Uncorrectable	100	100	0	0
188	Command Time Out	100	100	0	0
189	High Fly Writes	100	100	0	0
190	Airflow Temperature	63	60	45	623,181,861
194	HDA Temperature	37	40	0	37
195	Hardware ECC recovered	51	31	0	144,611,561
197	Current pending sectors	100	100	0	0
198	Offline scan UNC sectors	100	100	0	0
199	Ultra ATA CRC Error Rate	200	200	0	0
240		100	253	0	9,190
241		100	253	0	1,804,505,028
242		100	253	0	1,412,877,835

Elapsed: 0.3 sec.

Firmware looks fine

File System Structures

Found partition at sector 63 (type NTFS). Partition size: 104 GB.

Found partition at sector 204796620 (type Extended partition). Partition size: 395 GB.

Found partition at sector 204796683 (type NTFS). Partition size: 209 GB.

Found partition at sector 614389860 (type Extended partition). Partition size: 185 GB.

Found partition at sector 614389923 (type NTFS). Partition size: 185 GB.

Checking NTFS partition at sector 63. Partition size: 104 GB

Checking NTFS partition at sector 204796683. Partition size: 209 GB

Checking NTFS partition at sector 614389923. Partition size: 185 GB

Elapsed: 0.8 sec.

Partitions and file systems look fine.

(三)故障硬碟的檢測報告樣本如下：檢測的順序會依照前述的順序依次檢查，如前述報告樣本所示，Atola 會先檢查 PCB 板的狀況，本次檢測樣本因為係 PCB 板故障所以後續的磁頭檢測、媒體介面、韌體、檔案結構等檢查就不會進行，此時維修人員就可以針對 PCB 板進行維修，如此可減少維修人員判斷硬碟故障的部位，只針對故障的部分做檢修，本案例很明顯係 12V 電壓輸入有問題，故檢修人員可針對 PCB 板 12V 電壓處做檢視並維修。

Automatic Checkup finished

Report date and time: 2012/11/16 at 下午 02:46

Atola Insight v2.5.4423.31284

DiskSense unit: Ethernet

Device information:

Unknown device

Diagnostics results

The device has failed to initialize and become ready. Either circuit board or head stack are malfunctioning. More manual checking has to be done.

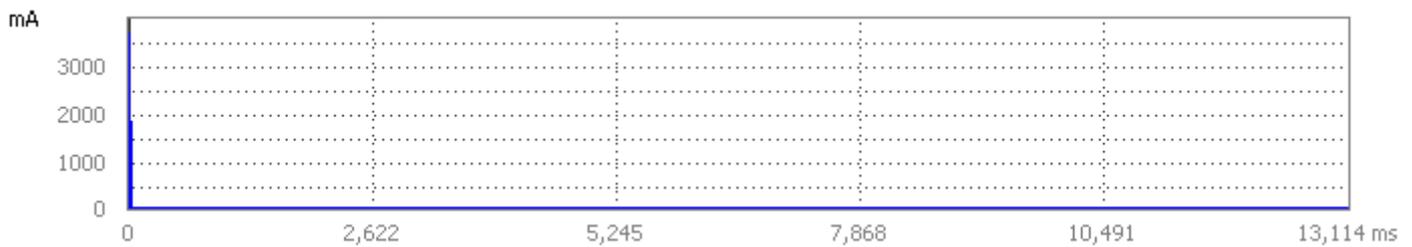
Full Diagnostic Log

Circuit Board (PCB)

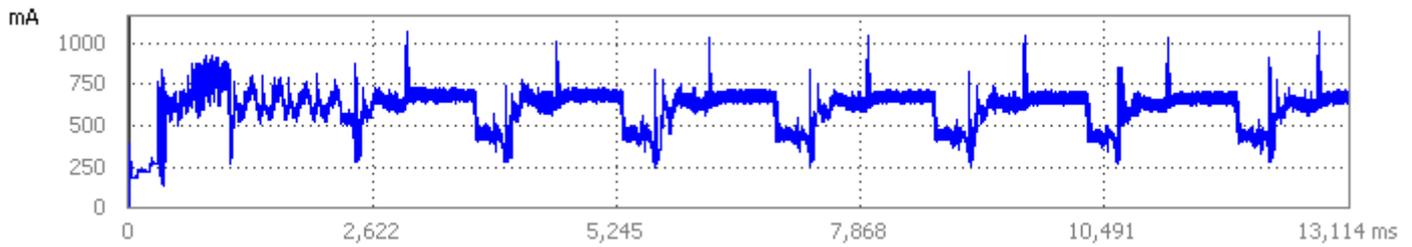
Selected Interface: SATA

Applying power and watching spin-up currents...

Current oscillogram (12V):



Current oscillogram (5V):



The device did not become ready in a timely manner.

Still waiting for the device - this may take up to 3 minute(s).

Device is still not ready

Registers: FFFF FFFF FFFF FFFF FFFF FFFF 8080 Alt: 8080

Peak power consumption during spin-up: 5V line = 1043.70 mA; 12V line = 3625.12 mA

Status register seems to be valid.

Device is still not ready. Resetting and waiting for 10 seconds...

The device has failed to initialize and become ready. Either circuit board or head stack are malfunctioning. More manual checking has to be done.

Heads

Head stack cannot be diagnosed.

Media Surface

Media test has been skipped because head stack test was not properly finished.

Firmware

Firmware cannot be diagnosed because of PCB damage.

File System Structures

File system test cannot be started.

(四)媒體介面掃描：媒體介面掃描可以瞭解磁頭存取的狀況，讀取的時間是否正

常，是否有壞軌的情形，此功能主要是可以瞭解磁頭損壞及硬碟磁盤損壞

的狀況。如下圖所示，紅框的部分顯示平均的讀取速度以及發生錯誤的區

塊，如此可以瞭解整個硬碟的存取情形，若損壞的區塊過多時，就建議即刻進行硬碟的 Image。

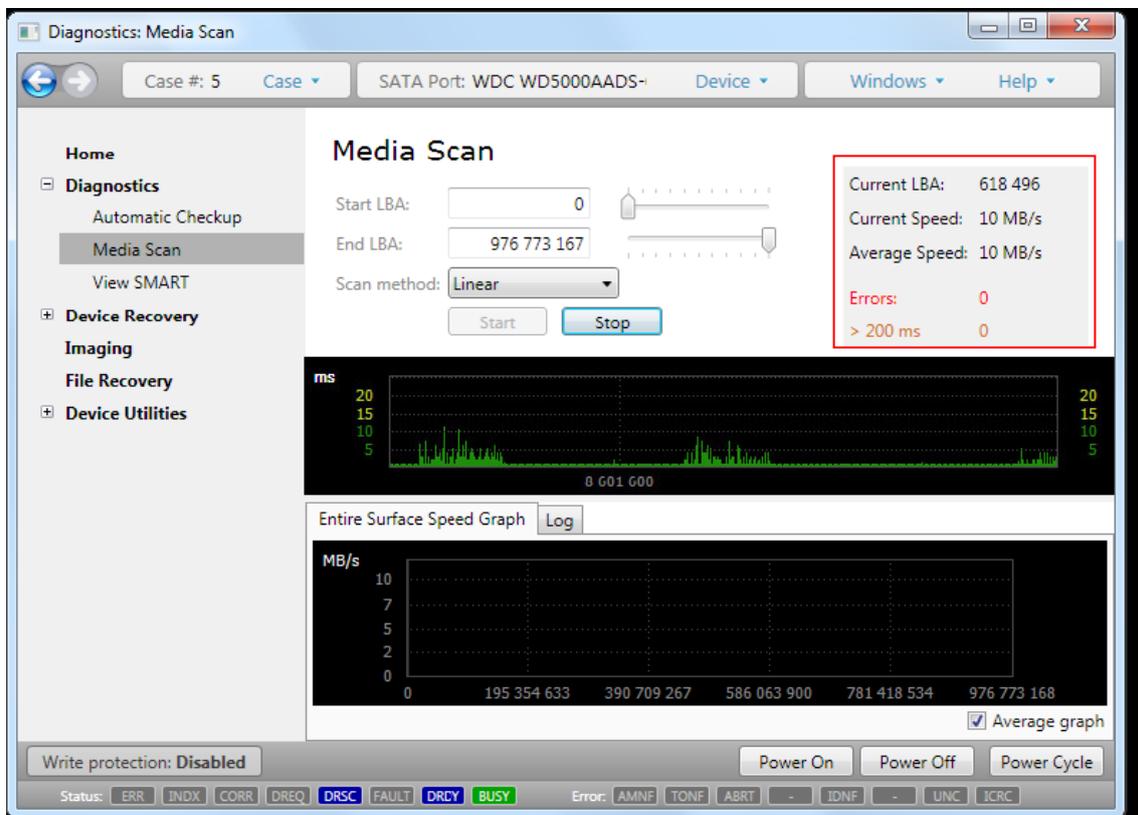


圖 3.4.3 Media scan 執行畫面

(五)韌體修復:Atola也提供韌體的修復，其中功能包括有韌體的備份（Firmware Backup），自動韌體修復（Automatic Firmware Recovery），韌體回存（Firmware Restoration），自動化的韌體修復只有針對某些有支援的廠牌及型號可進行修復，一般而言如果韌體有損壞時，可以把donor上的韌體先備份下來，再將備份的韌體內容回存到韌體損壞的硬碟上，但韌體裡面包含很多模組，有些模組是這一顆硬碟裡面獨有的，像是G-list、P-list、Translation Tables或是一些硬碟出廠時重要的參數，若是韌體損壞是這些重要的模組或參數，則該硬碟也無法修復。

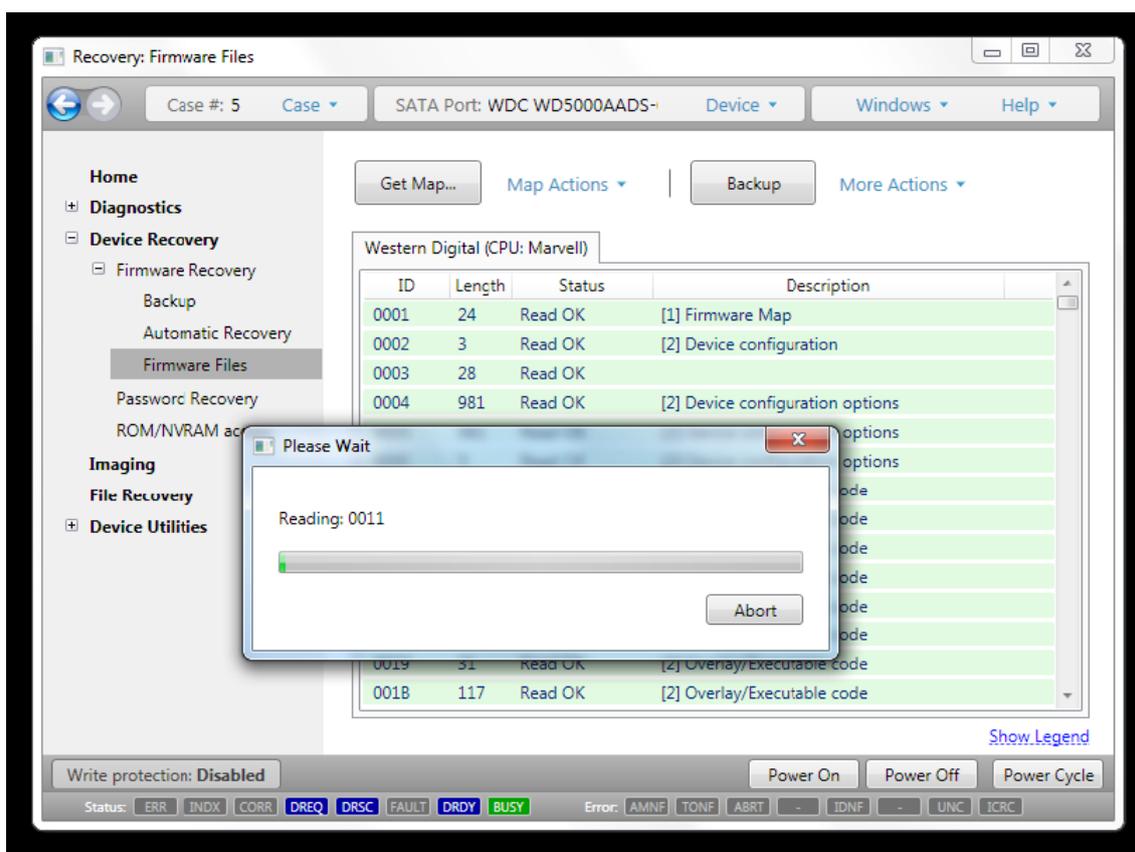


圖 3.4.4 韌體修復畫面

(六)分割區及檔案系統檢查:Atola 最後會檢查各個分割區的狀況，每個分割磁區 sector 的數量，與分割區的容量等資訊。

肆、心得與建議

一、**目標在資料救援而非硬碟修復**：現代社會已高度數位化，不論政府、企業及個人都脫離不了數位化的資料，而儲存數位資料目前最重要的媒體就是硬碟；硬碟是一種設備，有其使用年限，當硬碟突然不能正常運作時，就算資料仍儲存在硬碟內，亦無法存取運用，現今資料的價值往往超過硬碟本身許多，若該資料是唯一又重要的，那成功將資料救援的意義更遠大於將該硬碟修復，所以爲了將資料成功救援，硬碟本身是否能繼續使用，反倒是其次。

二、**毀損硬碟資料救援成功率不高**：硬碟本身的架構，主要包含外殼、印刷電路板、磁頭、磁臂、磁盤及馬達，還有出廠時內建的韌體模組及屬於該硬碟的唯一參數，如果毀損的部份是無可取代的部份，例如救援資料本身儲存的磁盤，或是唯一參數被毀損，就算有替代材料亦無法救回，另外就是在救援操作、更換零件之過程中的外在因素，例如電路板焊接偏移、過熱，落塵過多等，都可能導致救援成功率偏低，所以要提升資料救援之成功率，首先要提升人員之能力技術及經驗，再來就是要建置較佳之作業環境。

另毀損硬碟內之資料救援方法，不了解的人通常難窺其堂奧，總認爲需要高科技產品，如電子顯微鏡，生產硬碟之定位儀器等，且須在高等級之無塵室內操作，拆下硬碟磁盤透過最底層之磁力線讀取，還原成高階一般人可閱讀之資料，但這難度猶如要將已被碎紙機絞碎之紙片，還原

出紙張上的文字，就算能力可及，但所要花費之金錢時間及精神，應早已不符效益。

三、建立毀損硬碟資料救援能力之必要性：以司法案件之數位證據為例，在過去現場搜扣時，常發生硬碟過於老舊或被嫌犯當場將電腦泡入水中或摔毀，導致硬碟無法讀取，若未建立資料救援能力，只能求助於外界廠商，但又要考量案件資料的機密及敏感性(曾有涉及國家機密之案件)，不宜將硬碟送予民間廠商救援，所以政府機關自行建立毀損硬碟資料救援能力實有其必要，以應對證物硬碟遭無意或蓄意破壞。

四、固態硬碟或隨身碟之資料救援能力待提升：現今數位資料因成本考量，仍以硬碟為主要之儲存媒體，但隨著快閃記憶體等技術的成長及成本降低，將來以固態硬碟或隨身碟儲存資料的狀況會越來越多，而據統計此類媒體使用年限較硬碟更短，資料救援能力培養已刻不容緩。

五、資料救援人員能力宜專業化：毀損硬碟之資料救援除了一些外在環境因素會影響成功率外，操作人員對該型硬碟的了解程度、問題診斷及技巧純熟，也是成敗的關鍵，所以資料救援人員的經驗就像醫生一樣，需要不斷的累積案例經驗，而單位內如果不培養專人來負責救援任務，精益求精，則難以提升救援之成功率，遇到重要的資料待救援時，也無法有十足的信心。

六、毀損硬碟資料救援程序須納入鑑識程序考量：資料救援任務不宜全然依賴委外廠商的原因，除了硬碟內可能含有機敏資料之外，另外則是數位

鑑識程序之考量，正常運作的硬碟證物，鑑識程序會為其製作複本，然後在複本上進行分析，而非直接在證物上進行，但毀損硬碟無法如現行鑑識程序進行，需要改變取得證物時之原始狀態，所以建立毀損硬碟資料回復之鑑識程序，應是下一步重要工作。

附錄：附表及訓練照片

一、課程大綱

Day 1 1400~1630

<ul style="list-style-type: none">• Datarecovery Lab Standard and SOP
<ul style="list-style-type: none">• Datarecovery Lab Facility Introduction

Day 2 1000~1630

Getting Start with a full breakdown of hard drive anatomy and Basic Recovery Flow

<ul style="list-style-type: none">• Hard Driver Anatomy	<ul style="list-style-type: none">• P-List&G-List
<ul style="list-style-type: none">• S.M.A.R.T Data	<ul style="list-style-type: none">• Zone Table
<ul style="list-style-type: none">• Servo Information	<ul style="list-style-type: none">• Transalation Tables
<ul style="list-style-type: none">• HDD Firmware structure	<ul style="list-style-type: none">• Disagonsis procedure

Introduction to Atola Insight – Data Recovery Tools

<ul style="list-style-type: none">• Introduction Flow	<ul style="list-style-type: none">• Automatic Function
<ul style="list-style-type: none">• 4 Points of Data Recovery	<ul style="list-style-type: none">• Manual Function

Day 3 1000~1630

An Intense day packed with lectures, tutorials and practice session revolving around physical hard drive and clean room procedure.

Advanced Data Recovery Flow

<ul style="list-style-type: none"> • Proper HDD Diagnostics 	<ul style="list-style-type: none"> • Platter Swap
<ul style="list-style-type: none"> • PCB Recovery 	<ul style="list-style-type: none"> • Head Stack Issues
<ul style="list-style-type: none"> • PCB Replacement 	<ul style="list-style-type: none"> • Preamplifier issues
<ul style="list-style-type: none"> • Motor Issues 	<ul style="list-style-type: none"> • Error Prevention
<ul style="list-style-type: none"> • ATA Password Removal 	<ul style="list-style-type: none"> • HDD Firmware Recovery
<ul style="list-style-type: none"> • HDD Backup/Duplication 	<ul style="list-style-type: none"> • File Extraction

Diagnosis with Atola Insight-Data Rrcovey Tools

<ul style="list-style-type: none"> • Automatic Diagnosis 	<ul style="list-style-type: none"> • File Recovery
<ul style="list-style-type: none"> • Media Scan 	<ul style="list-style-type: none"> • Incorporation General Diagnostic

Day 4 1000~1630

Learn all you need know about data recovery with Atola Insight.

<ul style="list-style-type: none"> • Backup,Buplication &Imaging 	<ul style="list-style-type: none"> • Calibration Data
<ul style="list-style-type: none"> • Firmware Recovery 	<ul style="list-style-type: none"> • Case Management
<ul style="list-style-type: none"> • Password Recovery 	<ul style="list-style-type: none"> • Utility Function

二、訓練照片



圖 1 硬碟修復區



圖 2 硬碟收藏櫃



圖 2 現場上課環境



圖 3 實作示範

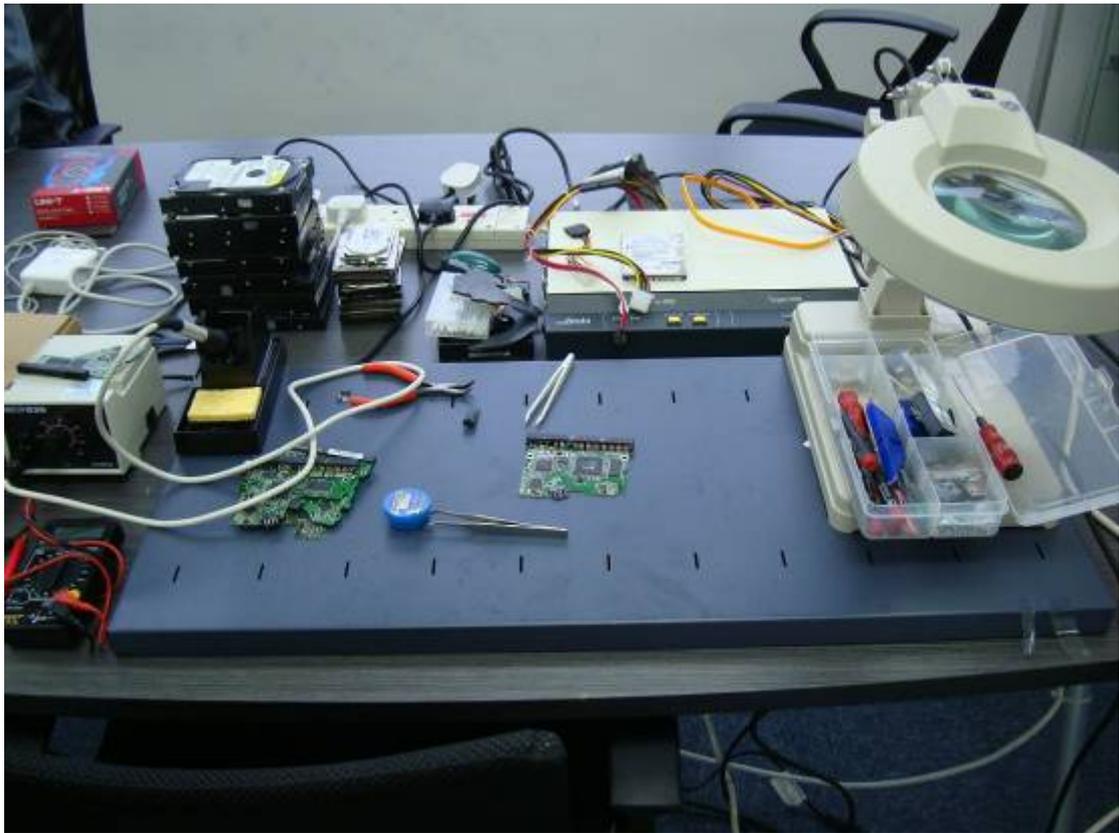


圖 4 各項修復工具及工作平台

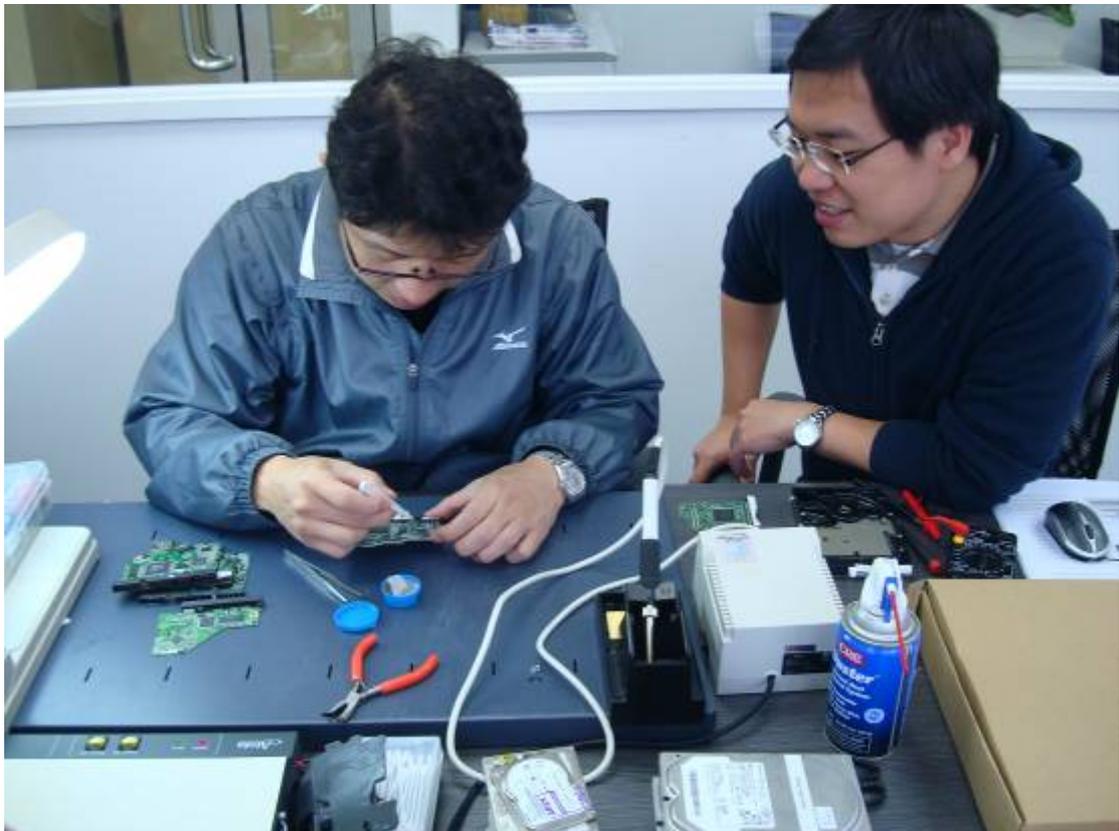


圖 5 實作練習