

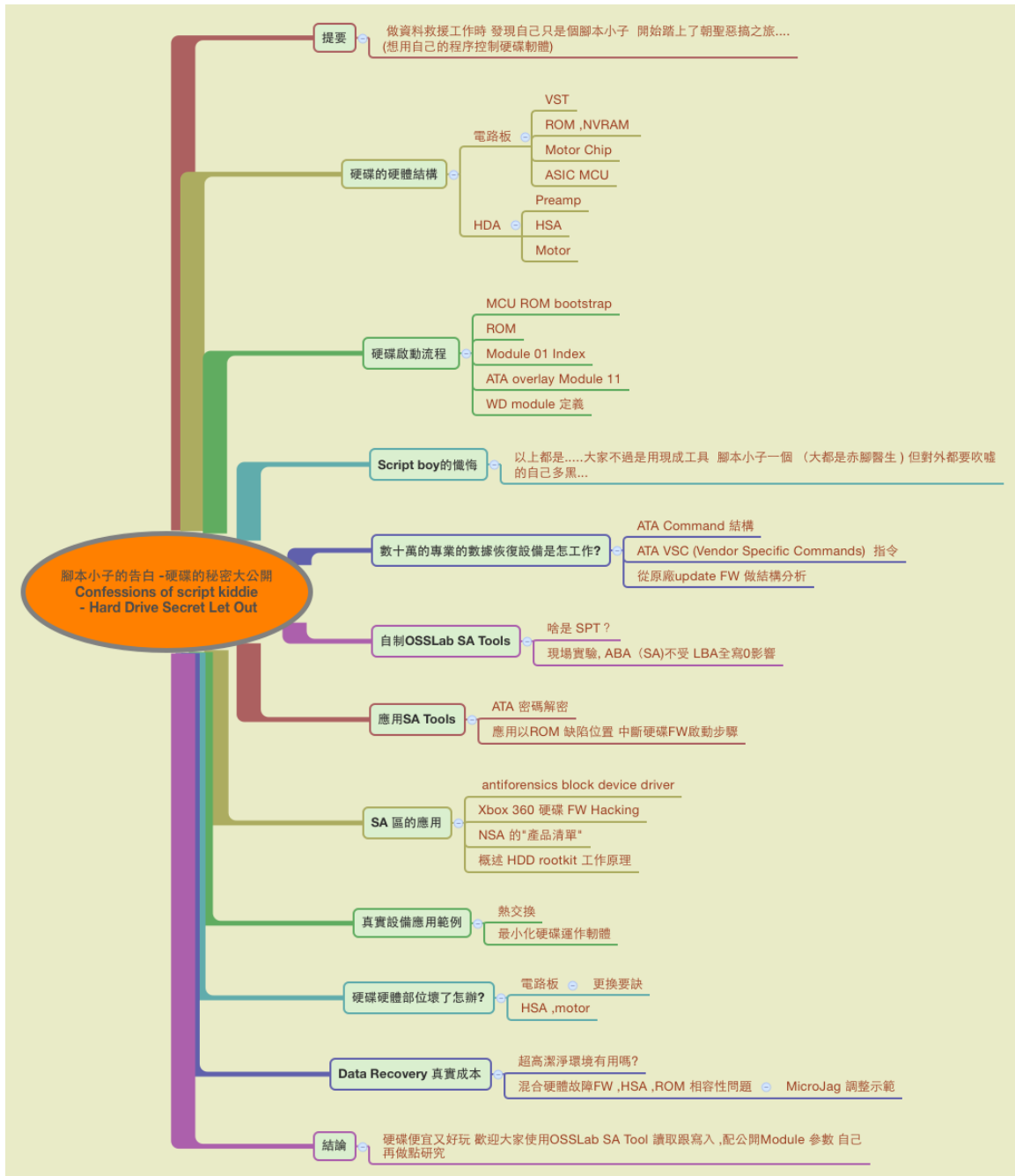
腳本小子的告白 -硬碟的秘密大公開

Confessions of script kiddie

- Hard Drive Secret Let Out

腳本小子的告白 -硬碟的秘密大公開 Confessions of script kiddie - Hard Drive Secret Let Out	1
1. 提要	3
1.1. 做資料救援工作時 發現自己只是個腳本小子 開始踏上了朝聖惡搞之旅... (想用自己的程序控制硬碟軟體).....	3
2. 硬碟的硬體結構	4
2.1. 電路板.....	4
2.1.1. VST.....	4
2.1.2. ROM ,NVRAM	4
2.1.3. Motor Chip.....	4
2.1.4. ASIC MCU	4
2.2. HDA	4
2.2.1. Preamp	4
2.2.2. HSA	4
2.2.3. Motor	4
3. 硬碟啟動流程	4
3.1. MCU ROM bootstrap.....	4
3.2. ROM.....	4
3.3. Module 01 Index	4
3.4. ATA overlay Module 11	4
3.5. WD module 定義.....	4
4. Script boy的懺悔.....	4
4.1. 以上都是.....大家不過是用現成工具 腳本小子一個 (大都是赤腳醫生) 但對外都要吹噓的自己多黑.....	5
5. 數十萬的專業的數據恢復設備是怎工作?.....	5
5.1. ATA Command 結構.....	5
5.2. ATA VSC (Vendor Specific Commands) 指令.....	5
5.3. 從原廠update FW 做結構分析	5
6. 自制OSSLab SA Tools.....	5
6.1. 啥是 SPT ?	5

6.2.	現場實驗, ABA (SA)不受 LBA全寫0影響.....	5
7.	應用SA Tools	5
7.1.	ATA 密碼解密	5
7.2.	應用以ROM 缺陷位置 中斷硬碟FW啟動步驟.....	5
8.	SA 區的應用	5
8.1.	antiforensics block device driver	5
8.2.	Xbox 360 硬碟 FW Hacking	5
8.3.	NSA 的"產品清單"	5
8.4.	概述 HDD rootkit 工作原理	6
9.	真實設備應用範例	6
9.1.	熱交換.....	6
9.2.	最小化硬碟運作軟體.....	6
10.	硬碟硬體部位壞了怎辦?.....	6
10.1.	電路板	6
10.1.1.	更換要訣.....	6
10.2.	HSA ,motor	6
11.	Data Recovery 真實成本	6
11.1.	超高潔淨環境有用嗎?	6
11.2.	混合硬體故障FW ,HSA ,ROM 相容性問題.....	6
11.2.1.	MicroJag 調整示範.....	6
12.	結論	6
12.1.	硬碟便宜又好玩 歡迎大家使用OSSLab SA Tool 讀取跟寫入 配公開Module 參數 自己再做點研究.....	6



1. 提要

1.1. 做資料救援工作時 發現自己只是個腳本小子 開始踏上了朝聖惡搞之旅...
(想用自己的程序控制硬碟韌體)

2. 硬碟的硬體結構

2.1. 電路板

2.1.1. VST

2.1.2. ROM ,NVRAM

2.1.3. Motor Chip

2.1.4. ASIC MCU

2.2. HDA

2.2.1. Preamp

2.2.2. HSA

2.2.3. Motor

3. 硬碟啟動流程

3.1. MCU ROM bootstrap

3.2. ROM

3.3. Module 01 Index

3.4. ATA overlay Module 11

3.5. WD module 定義

4. Script boy的懺悔

4.1. 以上都是.....大家不過是用現成工具 腳本小子一個 (大都是赤腳醫生)
但對外都要吹噓的自己多黑...

5. 數十萬的專業的數據恢復設備是怎工作?

5.1. ATA Command 結構

5.2. ATA VSC (Vendor Specific Commands) 指令

5.3. 從原廠update FW 做結構分析

6. 自制OSSLab SA Tools

6.1. 啥是 SPT ?

6.2. 現場實驗, ABA (SA)不受 LBA全寫0影響

7. 應用SA Tools

7.1. ATA 密碼解密

7.2. 應用以ROM 缺陷位置 中斷硬碟FW啟動步驟

8. SA 區的應用

8.1. antforensics block device driver

8.2. Xbox 360 硬碟 FW Hacking

8.3. NSA 的"產品清單"

8.4. 概述 HDD rootkit 工作原理

9. 真實設備應用範例

9.1. 熱交換

9.2. 最小化硬碟運作軟體

10. 硬碟硬體部位壞了怎辦?

10.1. 電路板

10.1.1. 更換要訣

10.2. HSA ,motor

11. Data Recovery 真實成本

11.1. 超高潔淨環境有用嗎?

11.2. 混合硬體故障FW ,HSA ,ROM 相容性問題

11.2.1. MicroJag 調整示範

12. 結論

12.1. 硬碟便宜又好玩 歡迎大家使用OSSLab SA Tool 讀取跟寫入 ,配公開Module

參數 自己再做點研究