Get rid of karma-Harkware hacking !

硬體駭客-解業障之路

OSSLab

前言

熱門的IoT資安,緊急狀況的資料救援,遊戲機破解,衛星訊號破解,FBI 未能解開的iphone.等

其實本質都是基於電子工程與資訊科學的軟硬相結合技術

且看OSSLab 分享實際案例硬體資安解業障之路.

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

不是這樣閒的當硬體駭客

為何要Hack硬體

不受原廠的限制.掌握系統權限,或是修改原廠所封鎖的限制,
方法手段:更換韌體,額外mod改裝,假送或攔截電子訊號協議等..

其目的通常如下：
1.好奇心:(研究 for fun,習慣root)
2.利益價值:(維修,盜版,資料救援)
3.特定用途:(國家利益)

OSSLab

1.好奇心 ,研究 for fun,習慣root

收費衛星節目，使用 CV12 共享盒，

這是電子協議relay破解

OSSLab

2.利益價值:維修,盜版

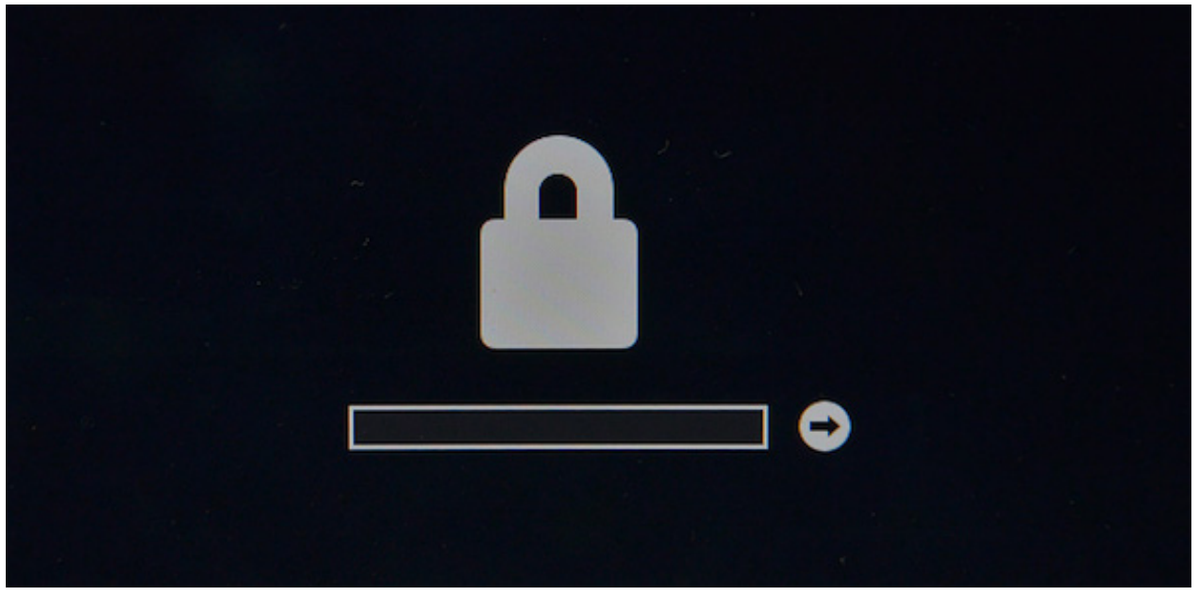
汽車

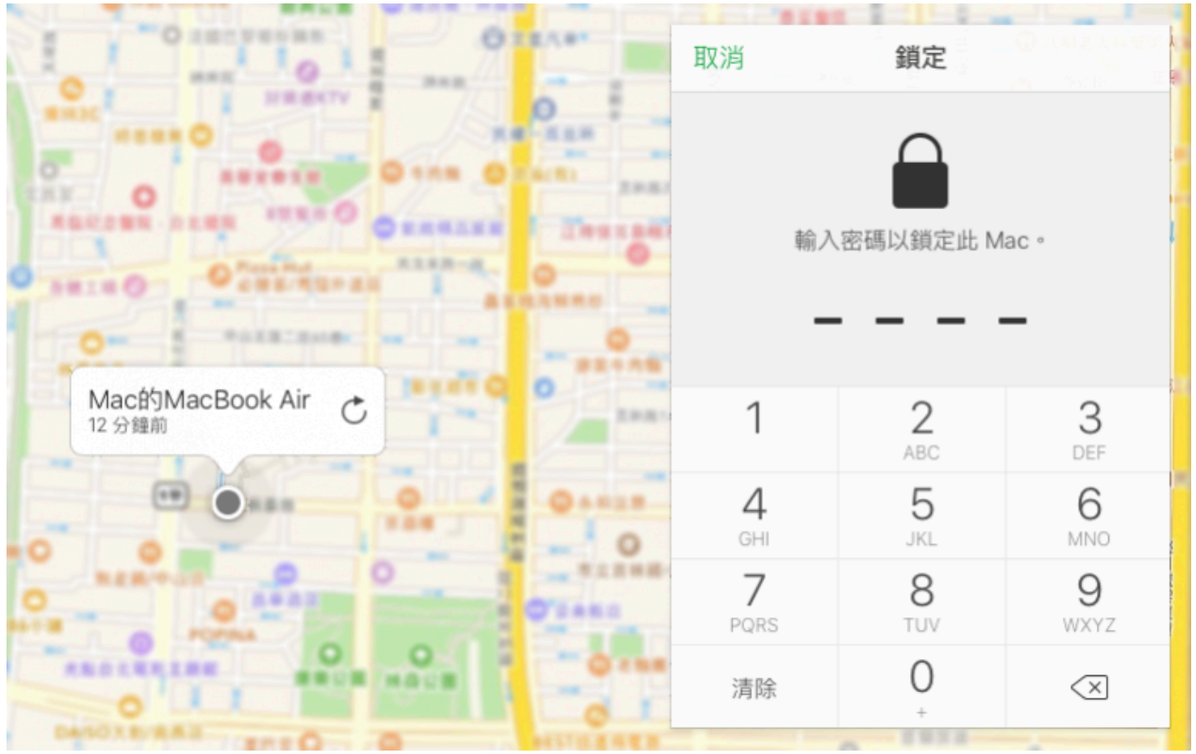
3. 利益價值

Iphone 5C

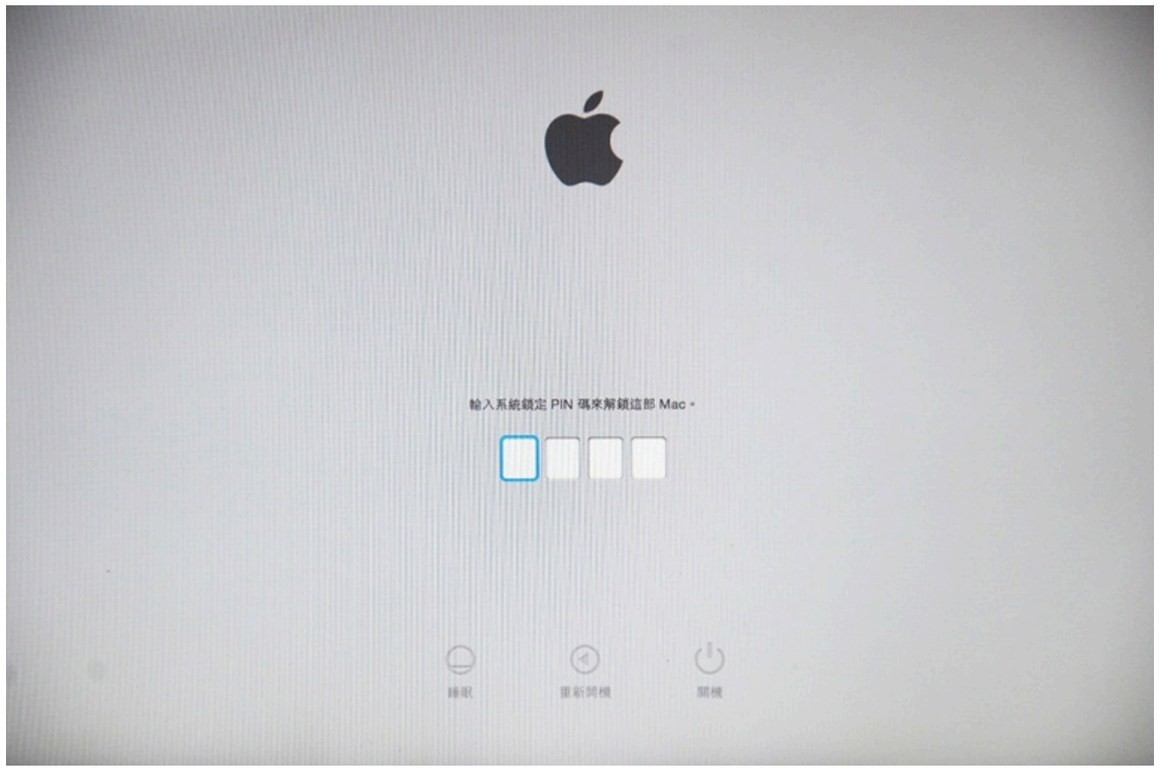
OSSLab

Macbook Efl破解





OSSLab



增加winhex 序號位置圖片 搜集一堆 bios圖片

OSSLab


概覽
顯示器
儲存空間
記憶體
支援
服務
macOS High Sierra
版本 10.13
MacBook Pro (13-inch, Early 2011)
處理器 2.3 GHz Intel Core i5
記憶體 16 GB 1333 MHz DDR3
啟動磁碟 Macintosh HD
顯示卡 Intel HD Graphics 3000 512 MB
序號 C17FGFZ5DH2G
系統報告⋯
軟體更新⋯
™ and © 1983-2017 Apple Inc. 保留一切權利。 許可協議

OSSLab

PC板卡破解

用IDA反組譯原廠工具韌體程式

讓原本OEM廠硬體 可以用原廠版本韌體https://marcan.st/2016/05/crossflashing-the-fujitsu-d2607/

OSSLab

修改使用時間 翻新與仿冒硬體

修改硬碟型號 ,通電時間,汽車里程

3.for 特定用途:

iot資安,

HDD與SDD Datarecovery:

從 泄露的工廠技術終端文件 破解
工廠指令集的原由:生產與維修

Live Demo 以終端指令 做Seagate ATA Password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

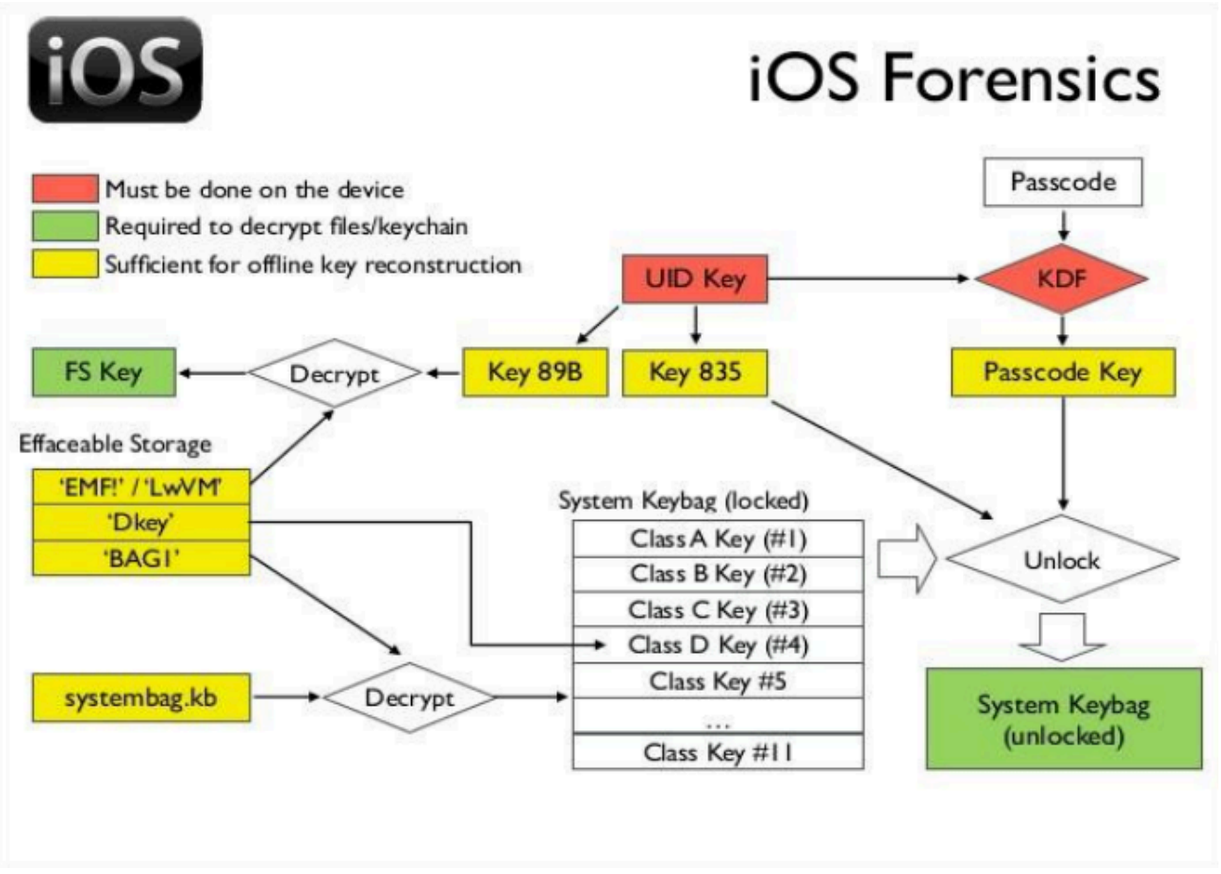
iPhone 5C NAND 鏡像攻擊

在此案例，公開演示了Iphone5C的工作原型和真實硬體鏡像的過程，雖然此過程仍可改進，但它仍然是一個成功的概念驗證項目。

此外，還揭示了Iphone 5C中NAND記憶體分配相關的一些可靠性問題。

OSSLab

IOS鑑識

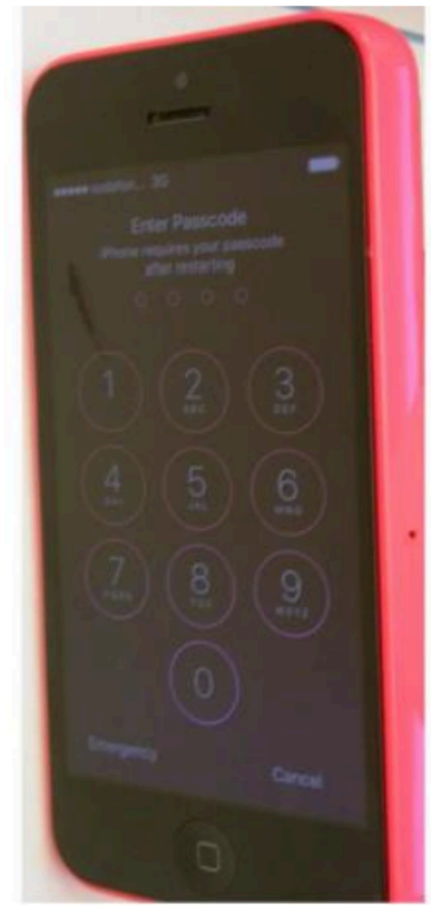


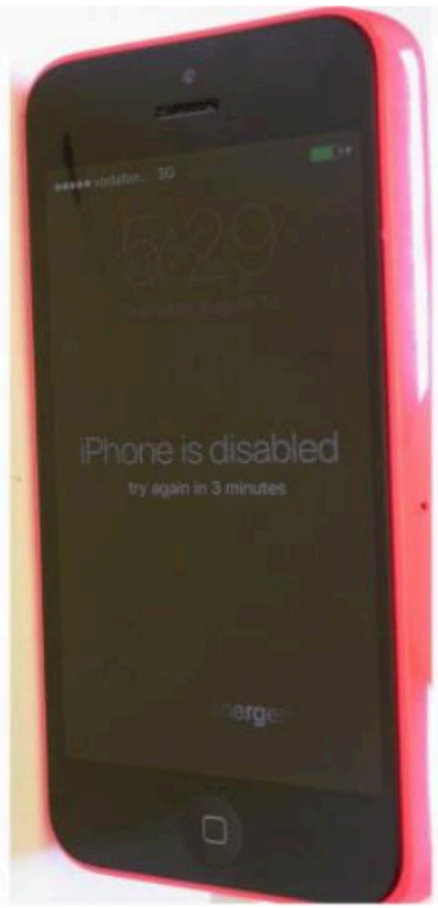
IOS的加密密鑰管理如圖所示，唯一的UID Key用於計算解鎖”System Keybag”的密碼密鑰。

UID Key被硬編碼在主SoC中，並且是CPU硬體安全引擎的一部份。

OSSLab

Iphone 5C 密碼安全性





若啟用安全性，啓動或喚醒時Iphone要求輸入密碼。

在連續5次不正確的嘗試之後，時間增加到1分鐘;然後5分鐘;10分鐘;最後60分鐘。

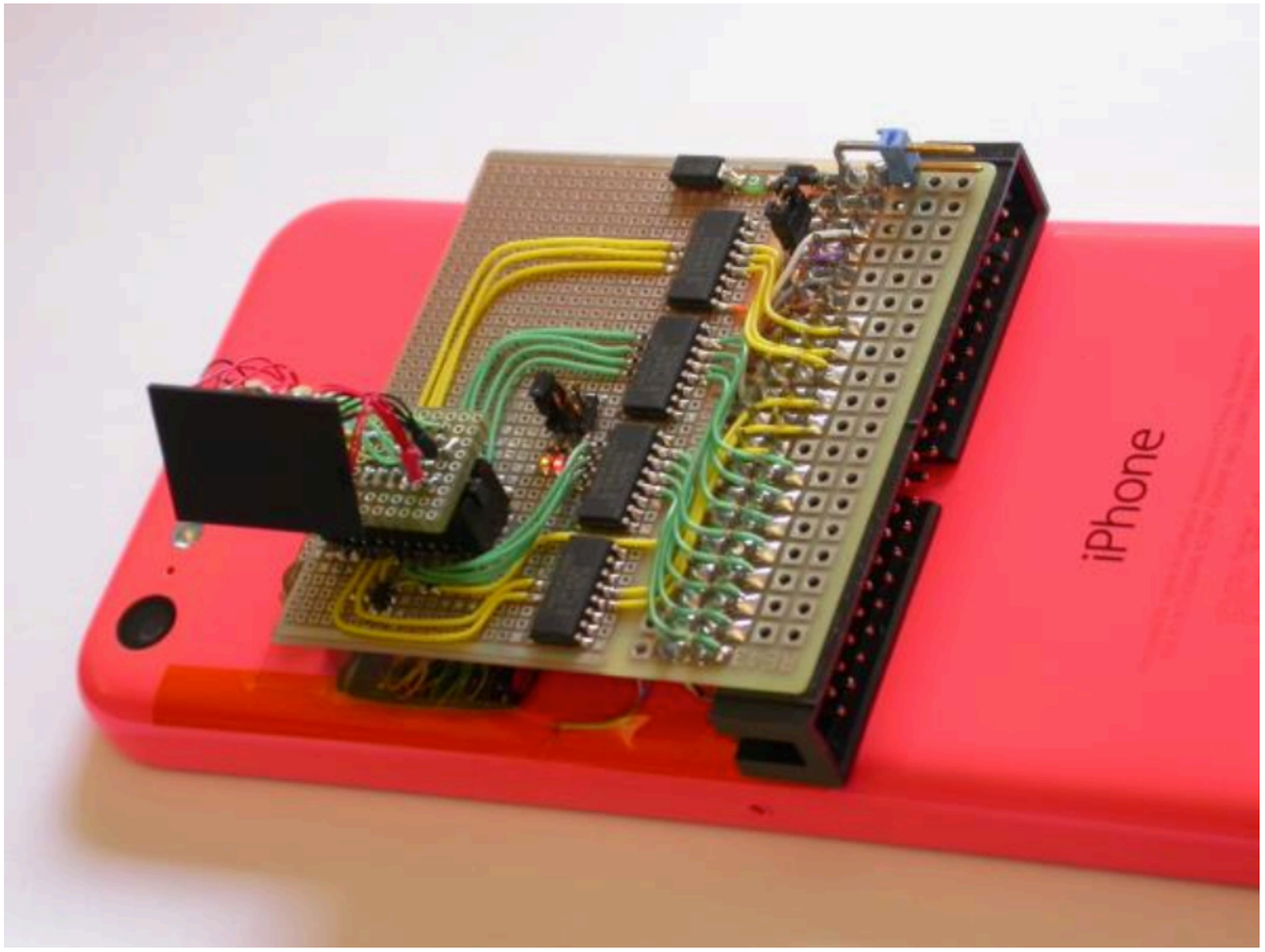
在連續10次錯誤後可選擇刪除所有數據。

OSSLab

NAND拆解後，為補助信號分析，連接到一個小型連接器。

匹配連接器焊接在主板上，跟NAND連接。

OSSLab



為了可靠竊聽，PCB版用緩衝器建成。

示波器及邏輯分析儀可用於訊號收集，毋須擔心探頭導線的高電容和低電組導致NAND通信信號過載。

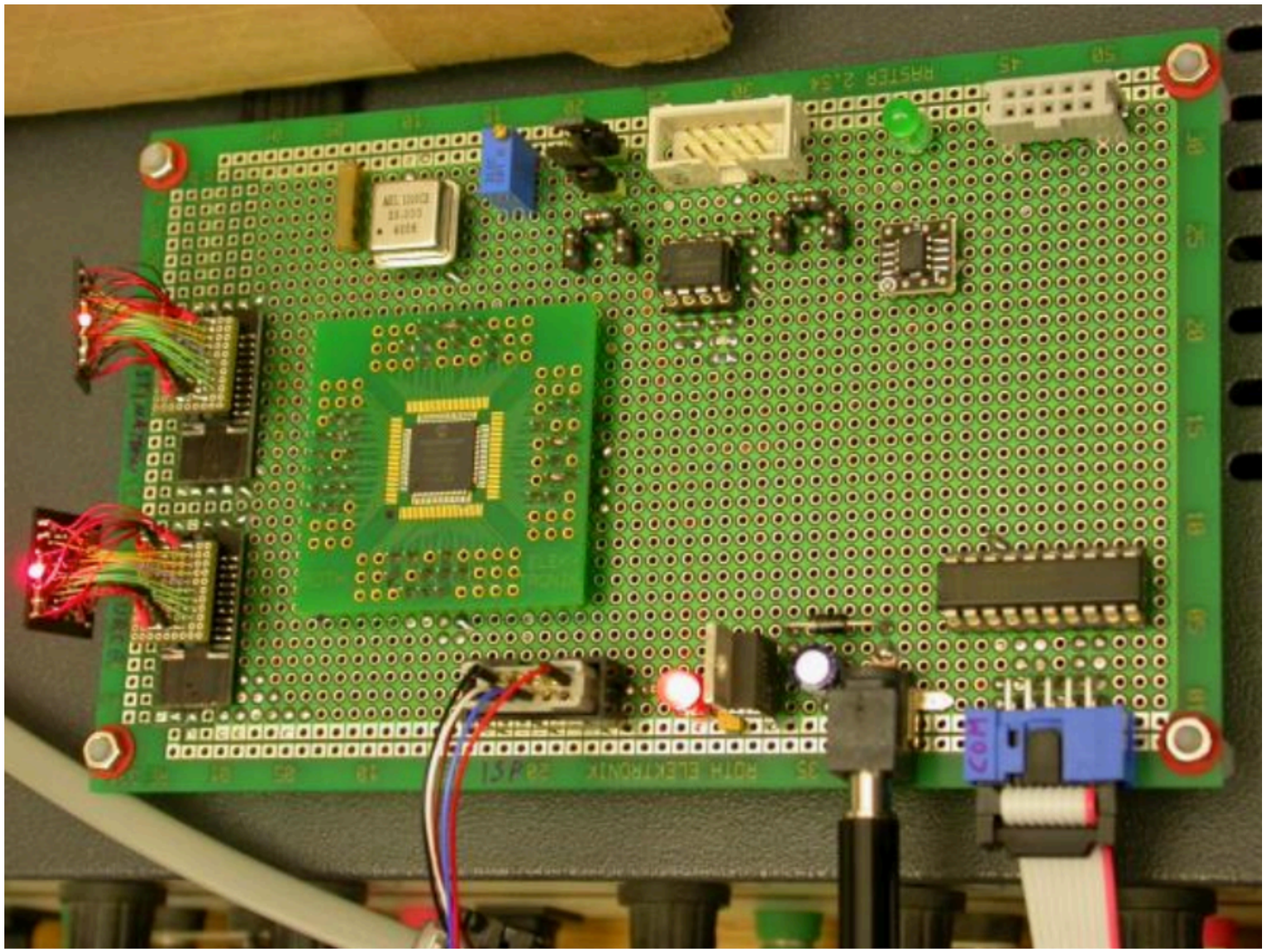
OSSLab

協議測試

為了調式所有用於NAND通訊的定制命令，製作一個簡易的適配器電纜，用於將帶有NAND晶片的中間板插入自製的通用編程器。

OSSLab

備份

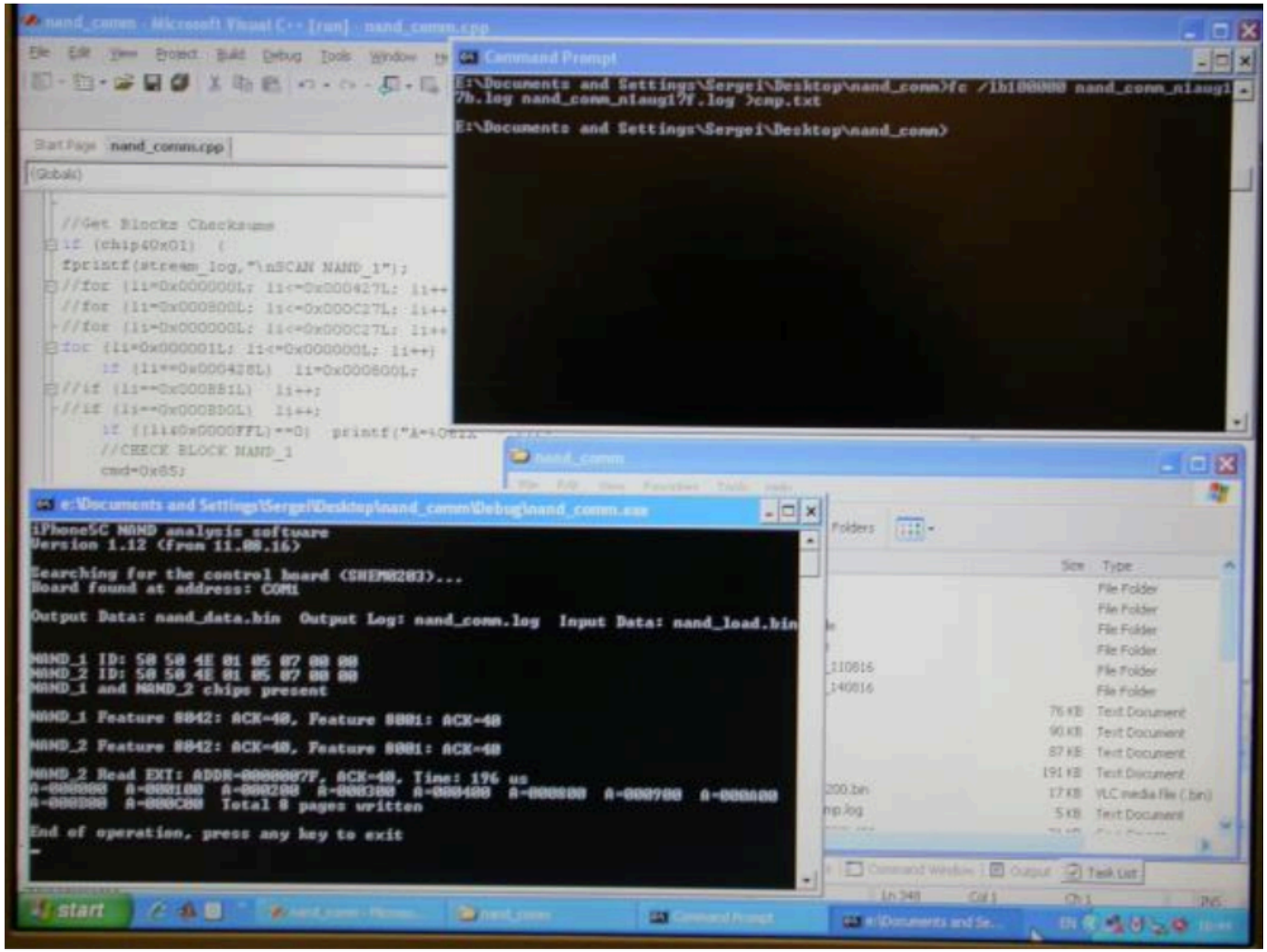


為了要創建NAND備份，建立一個基於硬體PMP接口，

Mircochip PIC24EP512GP806微控制器來當作此版核心。

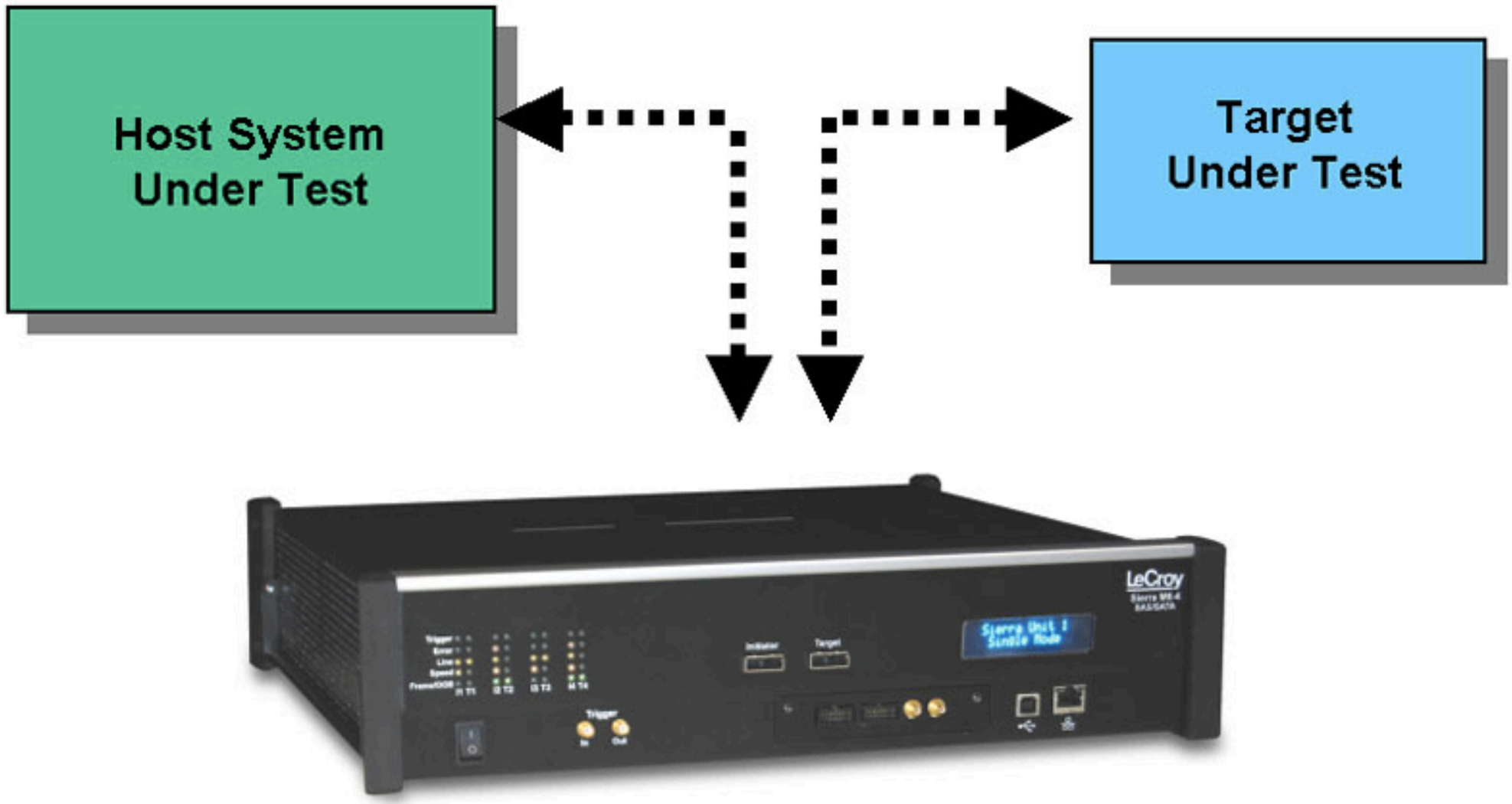
OSSLab

r


nand_comm - Microsoft Visual C++ [run] - nand_comm.cpp
Command Prompt
E:\Documents and Settings\Sergei\Desktop\nand_comm>fc /lb100000 nand_comm_ntaug1
7b.log nand_comm_ntaug1?f.log >cmp.txt
E:\Documents and Settings\Sergei\Desktop\nand_comm>
nand_comm.cpp
(Globals)
//Get Blocks Checksums
if (chip&0x01) {
fprintf(stream_log,"\nSCAN NAND_1");
//CHECK BLOCK NAND_1
cmd=0x65;
e:\Documents and Settings\Sergei\Desktop\nand_comm\Debug\nand_comm.exe
iPhone5C NAND analysis software
Version 1.12 (from 11.08.16)
Searching for the control board (SHEM0203)...
Board found at address: COM1
Output Data: nand_data.bin Output Log: nand_comm.log Input Data: nand_load.bin
NAND_1 ID: 50 50 4E 01 05 07 00 00
NAND_2 ID: 50 50 4E 01 05 07 00 00
NAND_1 and NAND_2 chips present
NAND_1 Feature 0042: ACK=40, Feature 0081: ACK=40
NAND_2 Feature 0042: ACK=40, Feature 0081: ACK=40
NAND_2 Read EXT: ADDR=0000007F, ACK=40, Time: 196 us
A=0000000 A=0000100 A=0000200 A=0000300 A=0000400 A=0000500 A=0000700 A=0000800
A=0000900 A=0000C00 Total 8 pages written
End of operation, press any key to exit
Folders
Size Type
File Folder
Text Document
VLC media file (.bin)
start

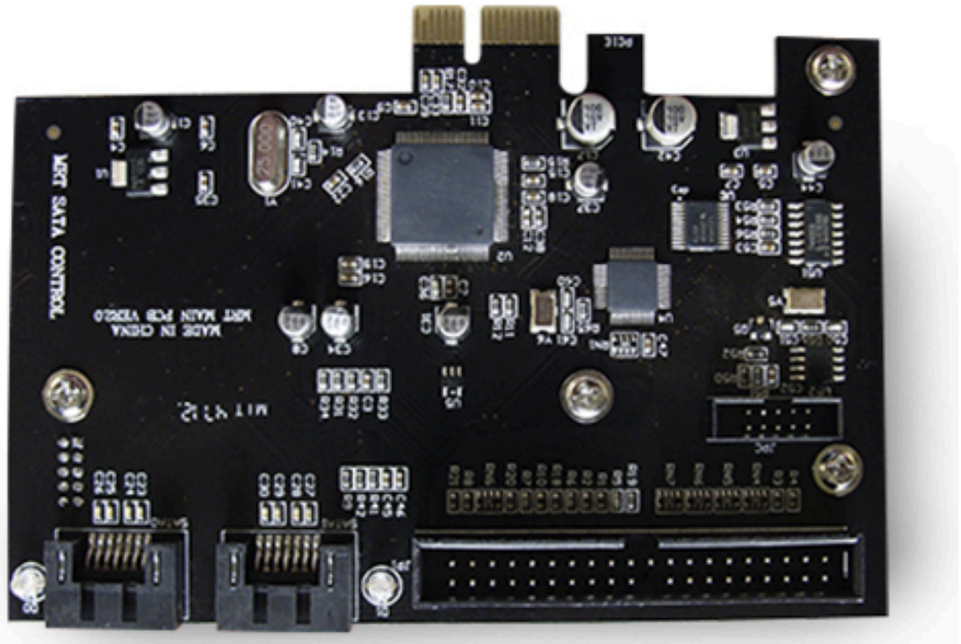
OSSLab

SATA 邏輯分析儀



OSSLab

資安硬體界的黑吃黑



OSSLab

整理上述的 example 手法 其實整理如下

1.弄到泄露的工廠技術文件指令集或電路圖,內部工具軟體,韌體升級軟體,非官方的
2.看懂電路圖,分類電子協議
3.Sniffer 電子協議
(SATA邏輯分析儀，跟其他邏輯分析儀)
4.物理Dump ROM ,NAND等.
5.分析 dump rom 或FW bin,通過IDA反組譯韌體 跟原廠工具程式 韌體升級程式
6.找到物理測試接口(JTAG)做動態反組譯
6..Fuzzy 窮舉可能的命令代碼

OSSLab

硬體容易被破解與入侵的狀況

1.未加密的bootloader
2.未加密Firmware (bootloader與檔案層)
3.未阻斷debug物理接點
4.fuse 未寫防止寫入或讀取 的 soc.
5.洩漏的工廠技術文件與程式
原廠工具軟體 韌體工具 韌體 沒有做好下面..
5.未防範Fuzzing 暴力破解
6.未加殼
7.未檢測中斷

OSSLab

如何做一名硬體駭客?

1.動手做最重要

2.好奇心

3.不懂就問或查資料.

OSSLab

Enjoy Hacking Hardware!

OSSLab