# ANALIZZARE DISPOSITIVI SENZA INTERFACCE O DISTRUTTI: LA "*CHIP-OFF*" FORENSICS

di Nanni Bassetti

## ❶ *Introduzione*

La tecnica d'indagine forense c.d "*chip-off*" rappresenta l'estremo tentativo di recuperare dati ed informazioni da un dispositivo, quasi sempre di tipo mobile (come ad es. il telefono cellulare, il *tablet*, la *pendrive*, il navigatore satellitare, l'unità GPS, la *game console*, il registratore digitale, ecc..), soprattutto quando non vi è modo di connettersi a causa della mancanza d'interfacce o perché il dispositivo è quasi totalmente distrutto. La tecnica del chip-off prevede, infatti, il distacco e l'estrazione del chip flash di memoria interno al dispositivo tramite la dissaldatura dello stesso.
Una tecnica meno invasiva del "*chip-off*" è l'acquisizione dei dati tramite porta **JTAG** (*Joint Test Action Group*), che permette ad un particolare *hardware* di connettersi alle porte JTAG del dispositivo, se presenti, e leggere i dati direttamente dal chip in esso contenuto. Questa tecnica richiede l'utilizzo dell'attrezzatura necessaria per aprire il dispositivo al fine di rivelare le porte JTAG, per effettuare un nuovo cablaggio, per collegare i fili appropriati dalle porte JTAG - *Test Access Ports* (TAPs) al *software* e all'*hardware* utilizzato per la lettura delle informazioni. Questa tecnica richiede, inoltre, personale specializzato e comporta difficoltà nell'interpretazione e decodifica dei dati come per il "*chip-off*" , pur essendo sicuramente preferibile poiché meno invasiva e non necessita di dissaldare alcunché, ma non è sempre applicabile.

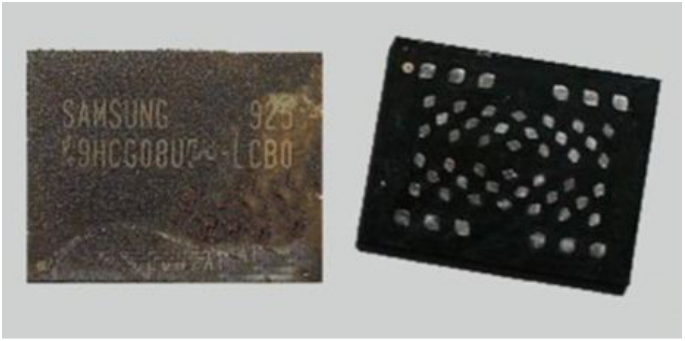
Quando tutto sembra impossibile ed ogni altra tecnica d'indagine forense fallisce o non è applicabile, si pensa al "*chip-off*". Vediamo però di seguito se la tecnica può essere considerata di facile applicazione e se fornisce ciò che si cerca.
Se prendiamo in esame il classico telefono cellulare, normalmente le informazioni contenute sono acquisite mediante *software* ed *hardware* specializzati, i quali riescono ad accedere alle memorie interne dei dispositivi ed effettuano il cosidetto "*dump*", generando *files* binari che poi vengono interpretati (*parsing*) e resi leggibili da sofisticati *software* d'analisi.

Per far tutto questo occorre connettere il telefonino tramite porte, cavi ed interfacce al *computer* o al macchinario dedicato, ma non sempre questo è possibile: a volte il dispositivo è completamente distrutto o danneggiato o non ha porte esterne di comunicazione, quindi la soluzione più razionale rimane effettivamente quella di dissaldare i chip e farli leggere da macchine dedicate.
Questa tecnica può esser applicata per estrarre dati da qualsiasi dispositivo che utilizzi una memoria di tipo flash (NAND, NOR, OneNAND o eMMC). I chip più comuni sono di due tipi, i TSOP (*Thin Small Outline Package*) ed i BGA (*Ball Grid Array*), i primi (TSOP) sono più facili da dissaldare per la loro morfologia, perchè hanno i piedini di connessione esterni attorno al bordo del chip, oltre che non richiedono la procedura di ricostruzione dei connettori. I chip BGA possono avere dai 40 ai 225 piedini distanziati a meno di 1mm tra loro.

Le fasi del "*chip-off*" sono tre:
1. dissaldamento dei chip,
2. *dump* del contenuto binario,
3. ricostruzione dei dati ed analisi.

## ❷ *Fase 1 - Il dissaldamento*

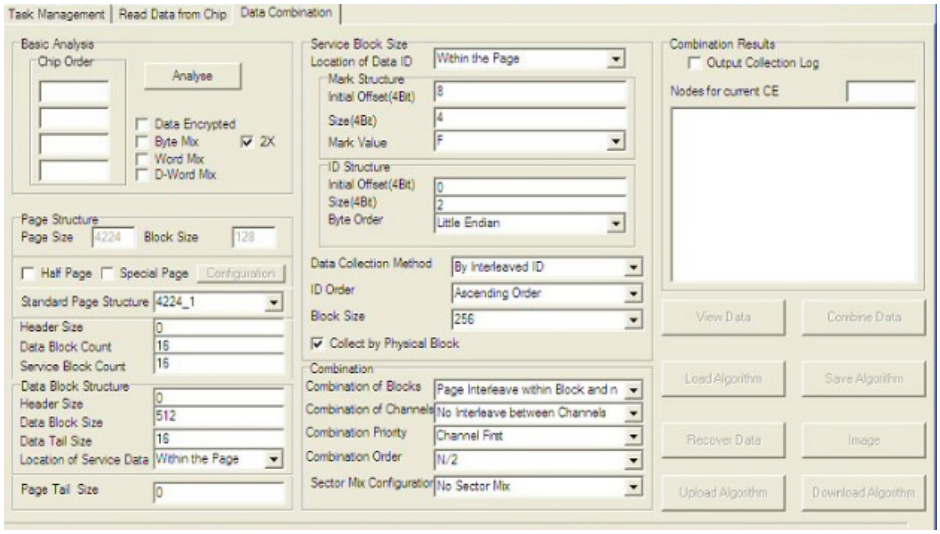
Il *chip flash* NAND (memoria) viene fisicamente rimosso dal dispositivo da una dissaldatura effettuata con attrezzature speciali che utilizzano un getto d'aria calda o una stazione a raggi infrarossi, e un strumento con effetto ventosa per rimuovere il *chip*.




Esistono anche tecniche che riscaldano il *chip* ad una temperatura specificata, però bisogna prestare attenzione e rivolgersi ad aziende specializzate perché è abbastanza facile danneggiare il *flash* NAND in questo processo.
Infine vi è la rimozione, che spesso danneggia i connettori sul fondo del *chip*, quindi deve essere prima pulito e poi riparato.
Il processo di riparazione dei connettori conduttivi sul fondo del chip BGA viene indicato come ***reballing***.

### ❸ *Fase 2 – Dump del contenuto binario*

Il *chip* viene inserito in un dispositivo *hardware* specializzato in modo che possa essere letto.
I dispositivi in genere devono essere predisposti per uno specifico circuito NAND *flash* e supportano una serie di *chip* noti. Terminato il *dump* si ottiene un'immagine fisica dei dati memorizzati sul *chip* NAND *flash*.




### ❹ *Fase 3 – Ricostruzione dei dati ed analisi*

La parte di ricostruzione del *file system* e dei dati è quella più complicata, perché legata agli schemi e strutture di memorizzazione delle informazioni sul supporto di memoria, oltre che a dover affrontare i problemi connessi al *wear leveling* meccanismo presente nei sistemi NAND. Al fine di allungare la vita delle celle di memoria della NAND, il *firmware* implementa algoritmi di *wear leveling*, ossia cerca di rendere il numero di scritture di ciascuna cella il più omogeneo possibile, in mondo da "consumarle" tutte allo stesso modo, poiché dopo un certo numero di scritture le celle perdono efficienza. Per questo tipo di gestione dell'informazione i dati non sono sempre sequenziali e facili da estrarre.

I *chip* NAND sono costituiti da un numero di "ERASE blocks" di una certa dimensione (comunemente di 128 Kb o 512Kb), ciascuno dei quali è diviso in un numero di pagine (da 512 bytes o anche 16Kb). Ogni pagina di flash NAND ha un "*out of band*" (OOB) Area per conservare l'*Error Correction Code* (ECC) e altri *metadati*, di solito 16 byte di OOB per ogni 512 byte di dati della pagina.

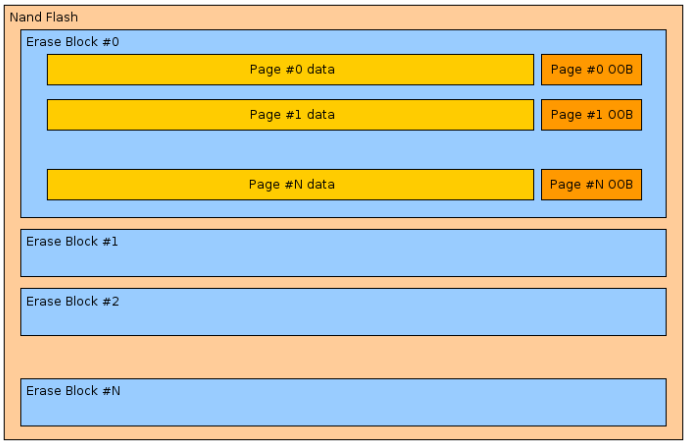



Immagine tratta da *http://techcorner.altenpts.nl/wp-content/uploads/2013/04/nand-flash.png*

Il blocco di memoria NAND deve essere cancellato prima che possa essere riscritto (da qui il nome ***Erase Block***); la dimensione dello spazio *out-of-band* dipende dal *chip*.
Una volta ottenuto il/i *file* binario/i, qualora non si riesca ad inserire i parametri giusti nel *software* di ricostruzione dell'informazione, tramite la ricerca di marca e modello, si dovrà agire tramite strumenti di basso livello utilizzati nella normale *computer forensics*, come l'estrazione di stringhe (ASCII, UNICODE, ecc.), il ***data carving***, la ricerca per parole chiave. Questo limita moltissimo la fase d'analisi poiché le informazioni estratte saranno spesso frammentate e di difficile comprensione. Infatti, nelle *flash memory* assieme ai dati sono presenti anche gli spazi "*spare*" (di riserva), le pagine sono sparpagliate e quindi, senza un riordino preciso, molti contenuti non saranno leggibili facilmente.

### ❺ *Conclusioni*

Anche se il processo di "*chip-off*" è molto efficace, le apparecchiature e gli strumenti necessari per applicare questa tecnica rappresentano una grande ostacolo per il loro elevato costo, inoltre devono essere utilizzate da un esaminatore con competenze molto specialistiche. Accanto a questi aspetti, rimane il rischio che il *chip flash* NAND sia danneggiato o si danneggi generalmente nella sua rimozione dal PCB (*Printed Circuit Board*).

I progressi nella decodifica ottenuti utilizzando gli strumenti commerciali per i *mobile device* ed i *software* per la *computer forensics*, e gli stessi strumenti di lettura di *chip*, sono migliorati continuamente.
In molti casi i risultati del recupero dei dati dalla memoria fisica dei dispositivi mobili è una massa di zeri e di uno o di dati esadecimali, che l'esaminatore ha bisogno di ritagliare manualmente e decodificare con altri strumenti, utilizzando la gamma di soluzioni nel *toolbox* di *computer forensics* tradizionale e *script* personalizzati per estrarre i dati.
Alcuni degli strumenti di *mobile forensics* sono utili per i dati acquisiti al di fuori del proprio supporto nativo, rendendo così più facile per l'esaminatore, lavorare ed implementare script personalizzati.
Infine, ricordiamo che il "*chip-off*" può esser utile anche per ritrovare dati su dispositivi protetti da *password*, ricavare piccoli artefatti come SMS, *web history*, *call logs*, stringhe di testo, ecc.., fatto salvo che l'informazione non sia stata criptata all'origine, altrimenti si ottiene solo una sequenza binaria incomprensibile.
Se invece si riesce a ricostruire il *file system*, tutto si vedrà come se si operasse su un normale *dump* "*bit a bit*" di un *computer*, fornendo informazioni che possono essere utili alle indagini. ©