

AIR

Automated Image

&

Restore

Release date	Author	Review	Note
V 1.0 08/03/2005	Michele Zambelli	Dario Forte	



Le procedure di Incident Response attuali prevedono, sempre, la duplicazione dei supporti originali compromessi o sospetti prima di qualsiasi attività di analisi. Nasce quindi l'esigenza di disporre di strumenti hardware e software efficienti in grado di duplicare con assoluta fedeltà qualsiasi flusso di dati da una sorgente a una destinazione.

Molte apparecchiatura hardware attuali permettono la generazione di tali immagini, dette in gergo "**Forensic Image**", in modo automatico, comodo e sicuro. Questi dispositivi funzionano autonomamente senza bisogno di nessun sistema operativo sottostante. Oltre a generare le immagini di diversi dispositivi:

- HD 3,5"
- HD 2,5"
- Device firewire
- USB Disk/Pen/Flash

permettono di calcolare il valore di hash MD5 o SHA1 dell'immagine originale e della copia prodotta stampando i report dell'attività.

Un esempio:



Forensic MD5 della Logicube.

Soluzioni ibride

Esistono soluzioni che fanno uso sia di dispositivi hardware, che funzionano da "**WRITE-BLOCKER**", ovvero inibiscono qualsiasi tentativo di scrittura del disco originale consentendone la sola lettura, sia di sistemi operativi minimali, spesso su CD, che gestiscono il processo di copia e di verifica di autenticità, ovvero il calcolo dei valori di hash.

Spesso tali dispositivi vengono collegati a sistemi che, per diverse ragioni, non possono essere aperti e quindi necessitano di un disco esterno come destinazione e di un sistema Microsoft o Linux che pilota i dischi durante la copia.

Soluzioni Software

Esistono tuttavia strumenti puramente software che permettono, con le dovute precauzioni, di raggiungere i medesimi risultati. Inoltre queste soluzioni possono essere estese ad altri ambiti delle attività forensi e non solo alla generazioni di immagini di dispositivi.

Il tool più diffuso e utilizzato attualmente per la gestione di flussi di dati è l'ormai noto **dd**. Nato come strumento di utilità per sistemi Unix si è affermato come standard certificato, nel campo forense, per la copia dei dati. In seguito sono nate delle modifiche di questo programma che ne migliorano l'utilizzo ai fini della sicurezza. Un esempio di questo è **dcfldd**, che oltre alla generazioni delle copie fornisce, a intervalli di blocchi prefissati, il valore MD5 del flusso di dati transitato.

Tuttavia questi strumenti necessitano di una buona conoscenza dei fondamenti di Unix e della loro sintassi. Generare la duplicazione di un disco e calcolarne il valore MD5 dell'originale e della copia richiede l'uso di due tool **dd** e **md5sum**, o di una soluzione unica come **dcfldd**, oltre a questo si aggiunge il fatto che tutto deve essere gestito da linea di comando.

Un esempio di copia di file e generazione dei rispettivi valori MD5:

```
# dd if=/mnt/hdb1/test skip=0 conv=noerror ibs=512 of=/mnt/hda1/test_copy seek=0
# md5sum test_file
# md5sum test_copy
```

Esempio d'uso di **dcfldd** per la generazione di una forensic image e relativo calcolo del valore di hash:

```
# dcfldd if=/dev/hda t skip=0 conv=noerror, sync hashwindow=0 hashlog=image.md5.txt
of=/mnt/hdb1/case/image.dd
```

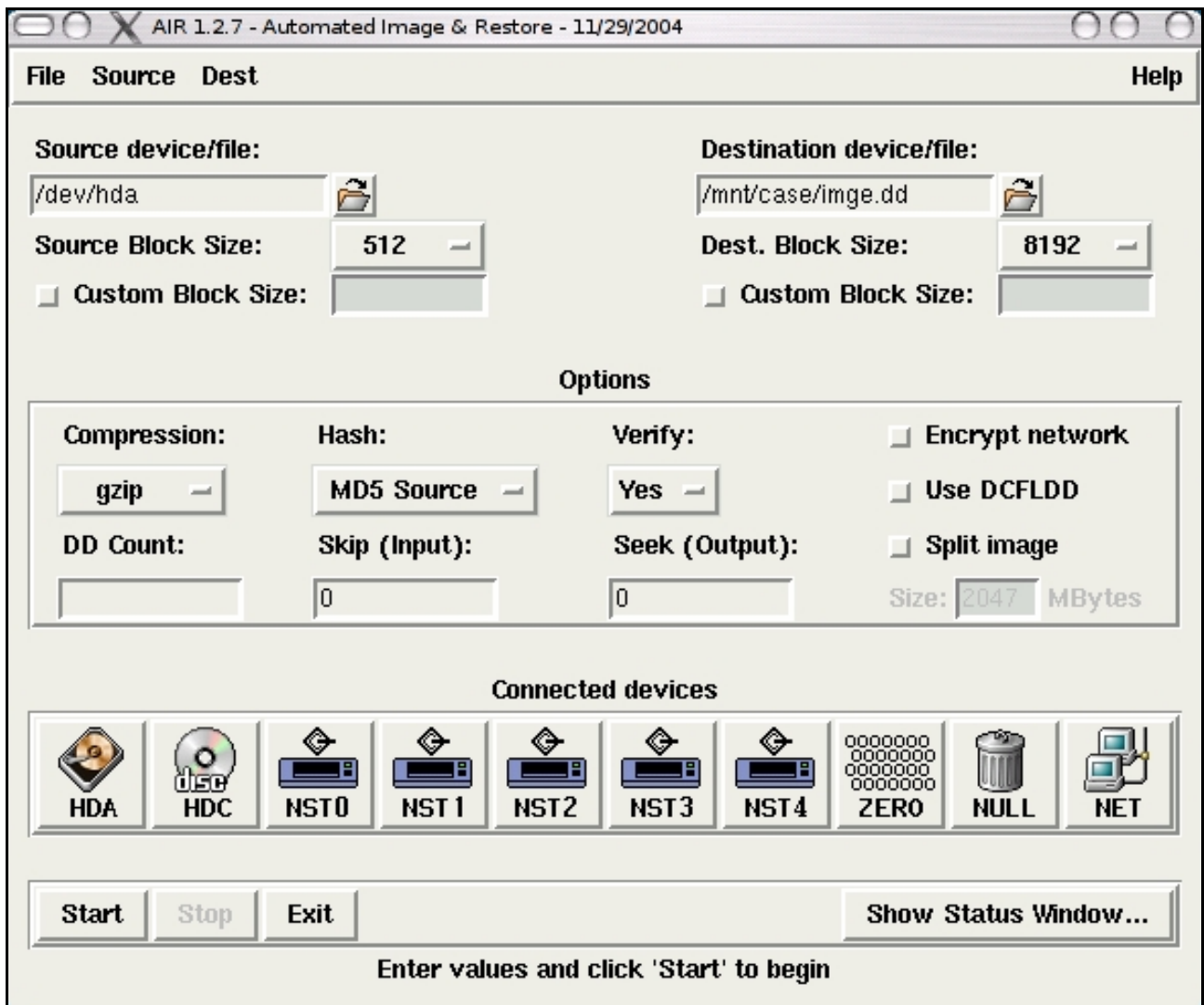
Quando si opta per soluzioni software è bene utilizzare dei dispositivi hardware detti "**Write Blocker**". Questi devono essere montati tra il disco originale e la forensic workstation. Il loro scopo è di impedire scritture accidentali sul disco sorgente.



AIR (Automated Image & Restore)

<http://air-imager.sourceforge.net/>

Questo strumento è un front end grafico per dd e dcfldd, inoltre fornisce molte altre funzionalità utili durante le procedure di duplicazione.



Al momento dell'avvio il tool riconosce, i device drive collegati al sistema siano essi IDE o SCSI drive, nonché i TAPE Device come presente in figura.

Per ogni disco rilevato è possibile ottenere un log, da allegare alla relazione finale dell'attività, con le specifiche tecniche dell'unità come nell'esempio:

```
/dev/hda:

Model=IC25N030ATMR04-0, FwRev=MOAOAD4A, SerialNo=MRG218K2HVAV4J
Config={ HardSect NotMFM HdSw>15uSec Fixed DTR>10Mbps }
RawCHS=16383/16/63, TrkSize=0, SectSize=0, ECCbytes=4
BuffType=DualPortCache, BuffSize=1740kB, MaxMultSect=16, MultSect=16
CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=58605120
IORDY=on/off, tPIO={ min: 240,w/IORDY: 120}, tDMA={ min: 120,rec: 120}
PIO modes:  pio0 pio1 pio2 pio3 pio4
DMA modes:  mdma0 mdma1 mdma2
UDMA modes: udma0 udma1 *udma2 udma3 udma4 udma5
AdvancedPM=yes: mode=0x80 (128) WriteCache=enabled
Drive conforms to: ATA/ATAPI-6 T13 1410D revision 3a:

* signifies the current active mode
```

Tra le Connected devices elencate troviamo anche:

- ZERO
- NULL
- NET

I primi due device vengono utilizzati per le operazioni di wiping dei supporti di destinazione, ovvero il completo azzeramento del loro contenuto. Questa operazione risulta indispensabile ai fini di una corretta duplicazione di un disco, infatti il supporto di destinazione non deve contenere nessuna traccia di dati non attinenti all'indagine in corso per non pregiudicarne la correttezza e validità.

Il terzo device permette la copia dei dati via rete, vedremo in seguito il suo funzionamento.

Duplicazione di un disco

Uno degli usi più semplici e comuni di AIR riguarda la duplicazione di device e quindi la scrittura, detta bit by bit, su un file di destinazione. Come avviene:

Supponiamo di avere a disposizione una **Forensic Workstation**(F.W.) per la duplicazione di un disco da sottoporre ad indagine, la prima accortezza da rispettare è quella di montare all'interno della F.W. i dischi nel seguente modo:

- **Disco Destinazione** (wiped), Device Master Primary Channel (/dev/hda)
- **Disco Originale** (Sorgente), Device Slave Primary Channel (/dev/hdb)

Questa disposizione riduce i rischi di scritture accidentali, nel momento dell'autodetection da parte del BIOS, sul disco originale o che il sistema al boot ne comprometta l'integrità.

Per questo motivo è meglio utilizzare, come ambiente di lavoro, un sistema operativo fidato di cui si conosce il processo di boot e che assicura che nessuna scrittura avvenga sui dischi installati. Per ciò è necessario impostare "**Boot CD only**" dal bios al momento dell'avvio del sistema.

Utilizzando un Live CD come Iritaly (www.iritaly.org) che dispone del tool AIR, e passando al momento del boot i seguenti comandi:

```
# knoppix noapm noswap dma
```

è possibile disporre di un sistema caricato interamente da CD e quindi fidato, che non modifica in nessun modo il contenuto dei dischi presenti nel sistema e che riconosce l'hardware presente nella macchina come device scsi e schede di rete.

L'opzione **dma** del boot è di fondamentale importanza in quanto riduce drasticamente i tempi di lavoro dei devices. Qualora dovessero presentarsi dei problemi al boot dovuti al caricamento del dma è possibile abilitarlo in seguito per ogni singolo dispositivo con il comando:

```
# hdparm -d 1 /dev/hda
```

I problemi di dma si possono riscontrare su periferiche vecchie.

In via preliminare è necessario montare il disco di destinazione **hda** in modo da disporre dello spazio necessario per la creazione del file destinazione. Un esempio del comando:

```
# mount /dev/hda /mnt/hda
```

La generazione dell'immagine avviene impostando come sorgente il device **/dev/hdb** dal menu di scelta di AIR e come destinazione il mount point e il file di destinazione da creare **/mnt/hda/hda_copy.img**.

Tra le opzioni di copia troviamo:

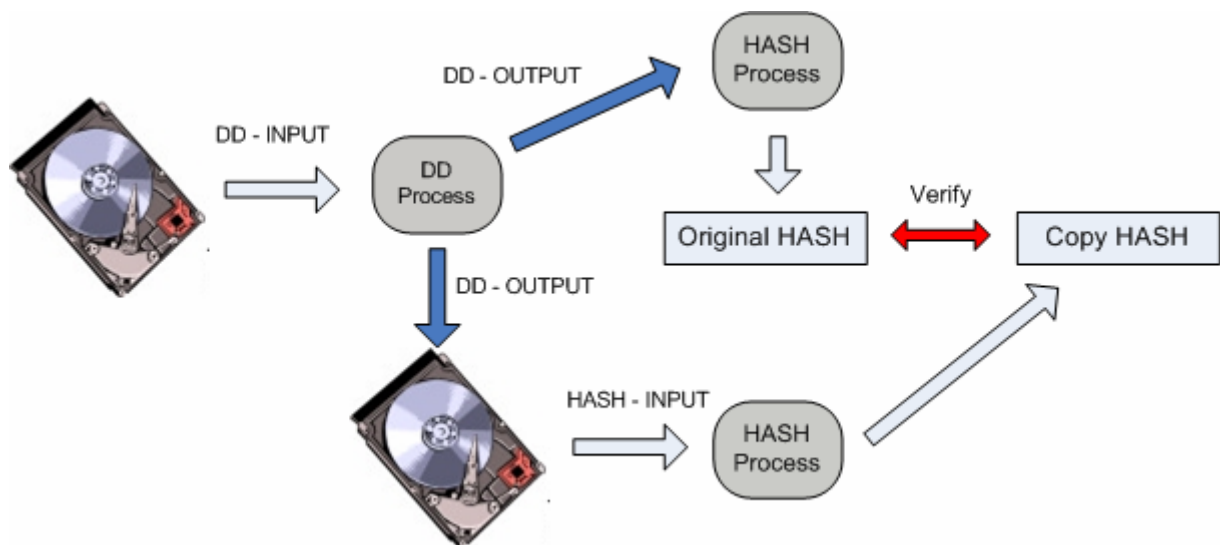
- Modalità di compressione
- Calcolo del valore di Hash
- Verifica della copia finale

Se si pensa di non disporre di abbastanza spazio sul disco di destinazione o si vuole creare un file di ridotte dimensioni per motivi di gestibilità è opportuno scegliere uno dei due algoritmi di compressione proposti, **gzip**, **bzip2**.

Il valore di hash da calcolare può, anche in questo caso, fare uso di due algoritmi **MD5** e **SHA1**.

A copia compiuta è possibile, se si usa l'opzione di verifica, confrontare il valore di hash calcolato sull'immagine originale con quello della copia prodotta per avere la certezza del buon esito delle operazioni.

Il processo di generazione delle copie dei dati e di calcolo dei valori di hash può essere così schematizzato:

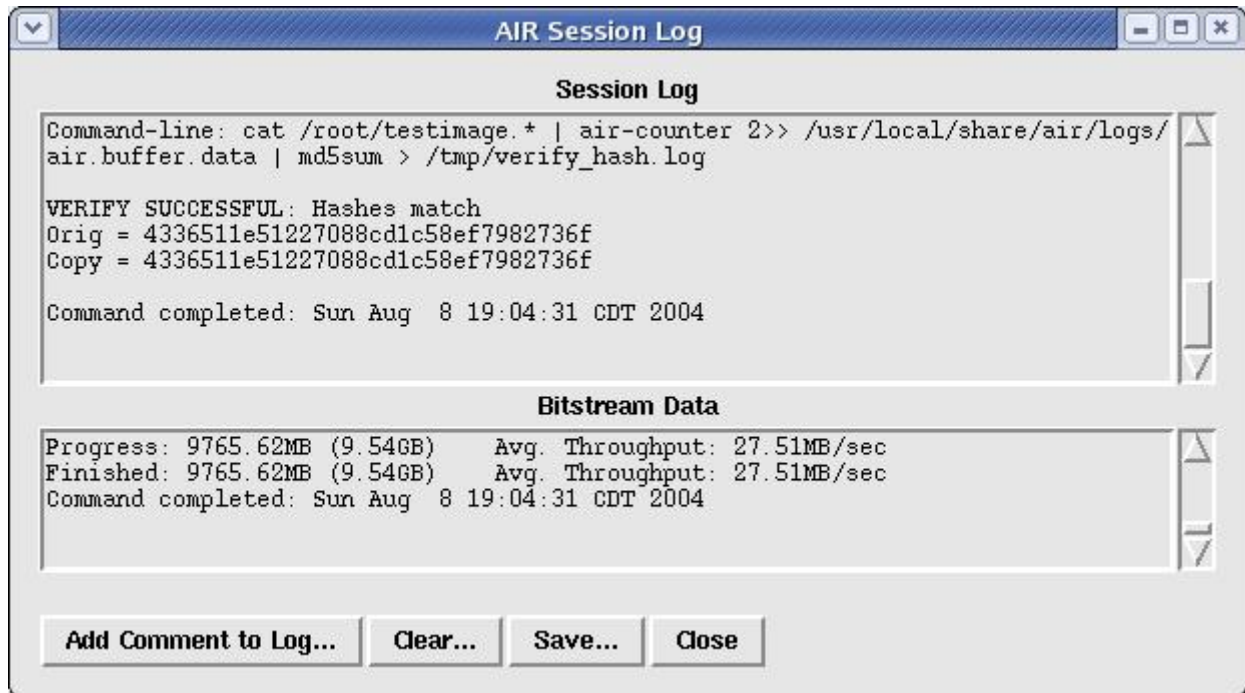


Usare la modalità **dcfldd** non varia il risultato finale del processo di copia ma utilizza questo strumento migliorato invece di dd.

Durante la copia dell'immagine può essere necessario suddividere in diversi file di dimensione prefissata l'immagine che verrà generata utilizzando l'opzione **split** e specificando la dimensione massima scelta. Tale dimensione di solito corrisponde alla capienza di un CD-R (640 MB) o di un DVD (4.7 GB) per motivi di gestione e archiviazione dei file.

Log

Tutte le operazioni che eseguite con AIR vengono loggate e presentate all'utente tramite la finestra di log.



Questa finestra oltre a fornire i dettagli delle operazioni compiute, con particolare riferimento ai comandi e alle opzioni utilizzate, fornisce un stima sempre aggiornata delle quantità di dati processate e delle velocità delle elaborazioni.

In ultimo luogo, a processo completato, stampa il risultato finale del calcolo dei valori di hash e delle copie di file.

I log possono essere modificati, salvati e allegati alla relazione finale.

Importante

AIR fornisce come log aggiuntivo l'output prodotto dallo strumento dd, è molto importante verificare che tutto sia andato a buon fine cioè che dd non abbia presentato degli errori di I/O durante i processi di copia.

Questo log risulta molto utile anche quando si intende copiare un normale file da una sorgente a una destinazione.

Se ad esempio disponiamo di un disco sul quale sono salvate le immagini dd, già generate, e vogliamo copiarle su un altro device, prima di procedere con le indagini, è bene, anche in questi casi, fare uso dello strumento AIR in quanto una semplice copia eseguita con il comando di Unix:

```
# cp <sorgente> <destinazione>
```

non permette di rilevare la presenza di eventuali errori di lettura o scrittura dei file.

L'utilizzo di AIR e quindi del tool dd migliora, tramite i log generati, la sicurezza che le copie siano andate a buon fine.

Un esempio di errore durante la compressione di una raw image:

Start DD: ven apr 1 15:52:42 CEST 2005

Command-line:

```
dd if=/mnt/hda1/img.raw skip=0 conv=noerror ibs=512 2>> /usr/local/share/air/logs/air.image.log |  
air-counter 2>> /usr/local/share/air/logs/air.buffer.data | gzip -1 | dd of=/mnt/hda1/copy_img.raw.gz  
seek=0 obs=8192 >> /usr/local/share/air/logs/air.image.log 2>&1
```

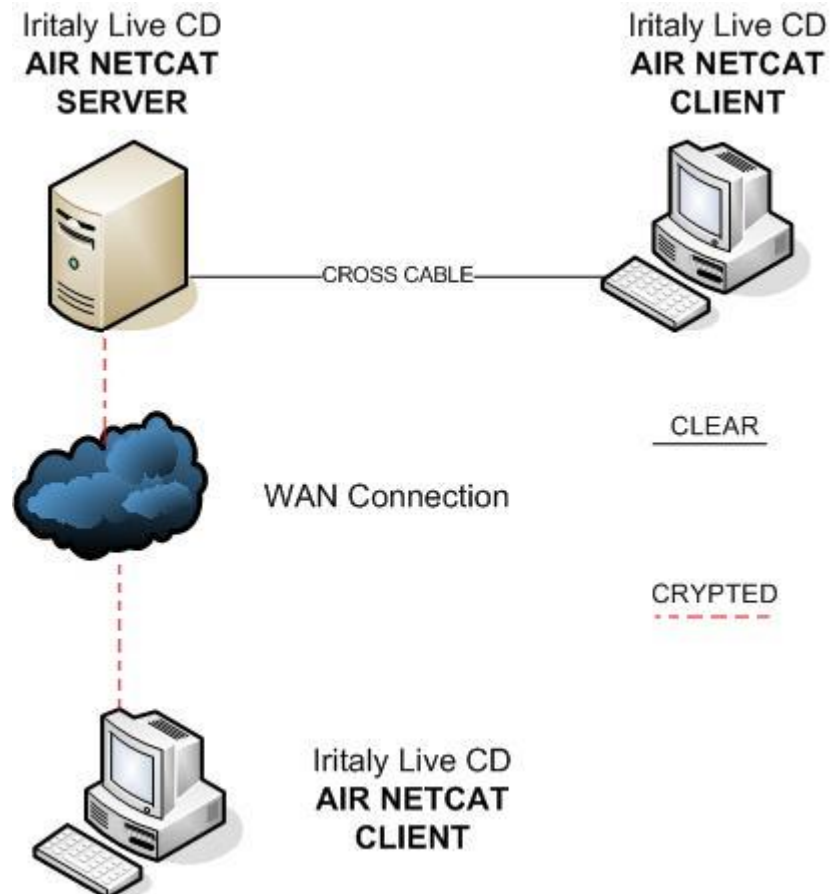
```
dd: reading `/mnt/hda1/img.raw': Input/output error  
13162976+0 records in  
13162976+0 records out  
6739443712 bytes transferred in 553,999413 seconds (12165074 bytes/sec)  
dd: reading `/mnt/hda1/img.raw': Input/output error  
13162976+0 records in  
13162976+0 records out  
6739443712 bytes transferred in 557,511238 seconds (12088445 bytes/sec)  
dd: reading `/mnt/hda1/img.raw': Input/output error  
13162976+0 records in  
13162976+0 records out  
6739443712 bytes transferred in 557,783253 seconds (12082549 bytes/sec)  
78165357+0 records in  
78165357+0 records out  
40020662784 bytes transferred in 2392,697215 seconds (16726171 bytes/sec)  
11281501+1 records in  
705093+1 records out  
5776128966 bytes transferred in 2394,387807 seconds (2412362 bytes/sec)
```

Command completed: ven apr 1 16:33:21 CE

Da notare che AIR integra i log con il time stamp di ogni operazione compiuta.

Copie via rete

In alcuni casi può risultare impossibile estrarre i dischi o spostare i sistemi da duplicare. AIR fornisce la possibilità di utilizzare un collegamento via rete, se disponibile, per la copia dei dati. Questa funzionalità è stata implementata usando lo strumento Unix *netcat*. Oltre a questo è possibile, per ragioni di sicurezza, criptare il traffico generato durante la copia, l'opzione è chiamata **Encrypt Network** che fa uso comando *cryptcat* di Unix.



Ovviamente è bene stabilire su quale porta dovrà avvenire la comunicazione e assicurarsi che un eventuale firewall presente su server o client accetti il traffico ad essa diretto.

Si consiglia tuttavia di effettuare le copie in questa modalità solo in casi strettamente necessari in quanto il traffico generato tende a congestionare la rete e aumenta notevolmente in tempi di tali operazioni.

Un esempio di configurazione di AIR:

Source device/file: port:66666	Destination device/file: /mnt/case/imge.dd
Source Block Size: 512	Dest. Block Size: 8192
<input type="checkbox"/> Custom Block Size:	<input type="checkbox"/> Custom Block Size: