Di **Michele Braga**

DATA RECOVERY

Cosa fare se si danneggia il supporto che contiene i dati della nostra vita in digitale: foto, video, documenti e file. Le tecniche di recupero dei dati.

I dati e le informazioni hanno un valore sempre più alto sia per le aziende moderne sia per i singoli individui. Nel primo caso sono strumenti indispensabili che devono essere trattati in modo corretto anche per assolvere ad obblighi normativi e che permettono all'azienda stessa di essere operativa e competitiva all'interno di un mercato sempre più veloce e globalizzato. I dati generati e accumulati dalle singole persone, invece, sono spesso più variegati, ma non per questo di minor valore: oltre a documenti con validità legale, la maggior parte dei dati – fotografie, video e scritti – attengono alla sfera affettiva, alle esperienze e ai ricordi personali.

Oggi la maggior parte dei dispositivi che utilizziamo – computer, smartphone, tablet, smartwatch, macchine fotografiche, action cam e così via – generano dati in forma digitale che teniamo sul dispositivo stesso o che più di frequente archiviamo su più supporti esterni e sul cloud, con lo scopo di parcheggiarli per consultarli in momenti successivi e per condividerli con altre persone. Questi supporti utilizzano tecnologie diverse e con il passare del tempo offrono capacità di archiviazione crescenti. A crescere non è solo la quantità dei dati generati, ma anche il peso dei singoli file: fotocamere con definizioni sempre maggiori generano file di dimensioni sempre più grandi, così come accade anche con i video in alta risoluzione.
Circondati da così tanti dati spesso non ci rendiamo conto di quanto siamo

KROLL ONTRACK

Da oltre 30 anni, Kroll Ontrack offre servizi e software all'avanguardia per assistere studi legali, aziende private, enti pubblici e utenti finali nella risoluzione delle problematiche e delle sfide poste dalla gestione dei dati. Parte di KrolLDiscovery, Kroll Ontrack fornisce soluzioni di recupero dati leader di mercato da hard drive, SSD, server, RAID, ambienti virtuali, cloud, dispositivi mobili, tape, NAS/SAN/DAS, computer laptop e desktop, device Apple. A livello internazionale KrolLDiscovery conta circa 1.300 dipendenti con presenza in 19 Paesi e 43 sedi. Kroll Ontrack è presente in Italia dal 2002 con sede in Gallarate (VA) dove si trova anche la camera bianca, l'unica professionale in Italia per il recupero dei dati. Inoltre, grazie alla tecnologia brevettata Ontrack Data Recovery Remote Services è possibile effettuare il recupero dei dati anche in remoto. La società sviluppa anche software per attività di recovery in autonomia: Ontrack EasyRecovery (per il recupero dati),

esposti – in modo inconsapevole o consapevole – al rischio di perderne anche solo una piccola parte in modo irrimediabile.
Con il termine irrimediabile non intendiamo infatti solo l'impossibilità di recuperare i dati persi, ma anche l'impossibilità di crearne di nuovi equivalenti. Un esempio calzante ed esplicativo può essere quello di una raccolta fotografica di un viaggio o di un evento come un matrimonio. Una volta perse le foto che hanno cristallizzato momenti passati, è piuttosto facile capire che non è possibile ricreare le stesse situazioni. Anche tornando a posteriori negli stessi luoghi degli scatti noi saremo cambiati, le persone e i luoghi saranno diversi così come le emozioni immortalate proprio in quegli scatti ormai persi.

Una vita in digitale

Un backup adeguato protegge i nostri ricordi digitali da perdite irrimediabili

Queste prime considerazioni ci portano per prima cosa ad affrontare lo spinoso tema del backup. Per quanto un utente dovrebbe sempre averne a disposizione almeno uno funzionante ed efficiente – il buon senso e l'esperienza consigliano di averne più di uno – esiste sempre la possibilità che anche il sistema di backup incorra in guasto. A tal proposito sottolineiamo che l'utilizzo di un Raid è spesso erroneamente considerata come una soluzione di backup; un sistema Raid ha lo scopo di garantire continuità di accesso alle informazioni in caso di guasti a un numero limitato di supporti che costituiscono il sistema Raid stesso, ma di per sé non rappresenta una soluzione di backup, ovvero la duplicazione di un file o di un'insieme di dati su un supporto esterno al sistema di lavorazione per averne una copia di riserva. Per questo e tanti altri motivi, chi tratta con dati digitali a scopo lavorativo e personale dovrebbe sempre possedere almeno un backup di quelli più importanti e che non possono essere ricreati.
I dispositivi sui quali archiviamo i dati sono di natura meccanica o elettronica e benché siano progettati e realizzati per essere longevi e resistenti, possono guastarsi completamente o comportarsi in modo non corretto. Tra le possibili cause che possono portare a ciò concorrono molti fattori, tra i quali dobbiamo annoverare anche l'errore umano. Utilizzando particolare attenzione e scegliendo dispositivi idonei allo scopo che devono svolgere è possibile ridurre la probabilità di incorrere in un evento che può portare alla perdita di dati, ma un simile evento deve essere sempre considerato come possibile.

Prima di andare oltre vale la pena di fare qualche altra puntualizzazione. La prima consiste nel precisare cosa si intende quando parliamo di "perdita di dati". Queste parole sono utilizzate molto spesso in modo improprio: "la perdita di un dato", da un punto di vista puramente letterale, significa che il dato stesso non esiste più e che quindi non è più recuperabile. In realtà, queste stesse parole sono utilizzate per indicare una "indisponibilità di un dato", ovvero l'impossibilità di accedere a dati che presumibilmente sono ancora presenti sul supporto dove sono stati archiviati.
Detto ciò, i dati possono essere inaccessibili per due motivi: fisici oppure logici. Nel primo caso si parla di un vero e proprio guasto al dispositivo

IL VALORE DEI DATI

Molti si rendono conto del valore dei dati solo nel momento in cui non sono più accessibili o solo quando sono definitivamente persi.
Una seconda considerazione, forse meno ovvia ma più importante, è che il valore dei dati non è un parametro sempre assoluto, ma in molti casi variabile: il valore di alcune informazioni, infatti, cala in funzione del passare del tempo. L'impossibilità di accedere a un'informazione per un tempo indeterminato può determinare l'inutilità dell'informazione stessa in quanto viene rimpiazzata da informazioni aggiornate.
Nel caso in cui si verifichi una perdita di dati è quindi importante dare un valore al dato stesso rapportandolo al tempo necessario per poterlo recuperare.
Ovviamente questo discorso non vale per tutti i dati: il valore di un archivio fotografico personale non diminuirà con il passare del tempo, perché i file in esso contenuti hanno congelato un momento specifico di una nostra esperienza di vita e non possono essere ricreati o sostituiti in alcun modo.

Paolo Salina
Country Director Kroll Ontrack Italia

Ontrack PowerControls (nelle versioni per il mailbox management in Microsoft Exchange Server, per il document recovery in Microsoft SharePoint Server e per il restore di singole tabelle in Microsoft SQL Server). Infine, Kroll Ontrack fornisce servizi di ediscovery, soluzioni per la gestione dei tape e per la cancellazione sicura attraverso il dispositivo Ontrack Eraser Degausser e i software Blancco, di cui l'azienda è distributor e gold reseller.
Per maggiori informazioni *www.krollontrack.it*

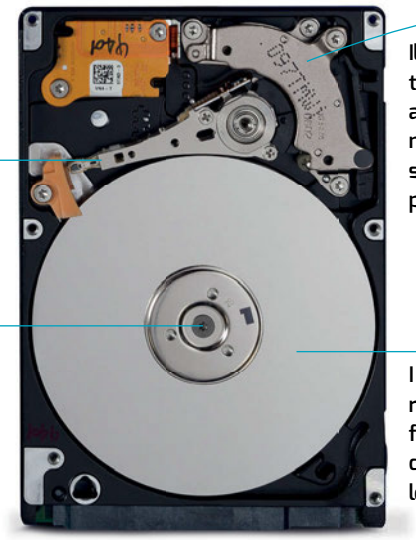
che contiene i dati, mentre nell'altro si fa riferimento a un problema che riguarda la struttura dei dati e che ne preclude l'accesso, come ad esempio a seguito della corruzione del file system.
Ancora, possiamo dire che i motivi principali che possono portare all'indisponibilità o addirittura alla perdita effettiva dei dati sono due: la sottovalutazione del rischio e un evento imprevisto. In ogni caso, quando si perde la capacità di accedere ai dati non è detto che le speranze di un recupero siano nulle. Se i dati sono fisicamente presenti, cioè non sono stati sovrascritti o il supporto fisico non è seriamente e irrimediabilmente danneggiato esiste una concreta possibilità di recuperare tutto o una parte del contenuto. In questi casi può essere necessario ed è consigliabile affidarsi a servizi specializzati in grado di operare sul dispositivo danneggiato che contiene i dati, per tentare di recuperare e ripristinare i dati stessi.

L'esplosione degli archivi dati personali sia per numero sia per dimensione di dati contenuti ha generato un'ampia e molto variegata offerta di servizi dedicati al recupero dei dati persi; basta una ricerca sui principali motori di ricerca Internet per essere inondati da innumerevoli annunci relativi a recuperi dati "sicuri", "garantiti" e spesso con prezzi "irrisori" per chi conosce quale sia il lavoro che può comportare un tentativo di recupero dati. Chiariamo subito una cosa: il recupero dati da un supporto danneggiato è un'operazione estremamente delicata che può avere esiti diversi in base al tipo di guasto. Finché un esperto non analizza il supporto e valuta l'entità del danno è impossibile sapere se si potrà recuperare qualcosa o meno. Di conseguenza diffidate da chi, anche in buona fede, vi assicura un recupero completo delle informazioni: spesso i risultati e i costi non sono assolutamente quelli attesi e, se il supporto viene smontato e utilizzato con tecniche di recupero inadatte, anche il suo successivo invio a seri professionisti del settore può essere ormai inutile. Ricordate bene, **il primo intervento è quello decisivo** come ci ha sottolineato anche Paolo Salin, Country Director di Kroll Ontrack Italia, con il quale abbiamo avuto modo di approfondire le tematiche di questo settore e che ci ha supportato a livello pratico e tecnico per seguire le fasi di un recupero dati reale.

SUPPORTI E PROBLEMATICHE

Quali sono le principali cause di guasto a un disco o più in generale a un supporto dati? Quali sono le differenze tra un supporto e un altro?

Come abbiamo già accennato, la varietà degli eventi che possono portare al malfunzionamento o al guasto di un supporto per l'archiviazione dati e alla conseguente impossibilità di accedere alle informazioni in esso contenuti è così vasta che risulta impossibile stilare una casistica esauriente, anche affidandosi alla più fervida immaginazione.
Quello che possiamo fare, invece, è sfruttare la statistica, individuando così le principali cause di danneggiamento. Rispetto a quando erano presenti prevalentemente unità meccaniche, oggi il panorama dei supporti è molto più ampio e diversificato. Ai dischi rigidi di tipo meccanico (HDD) si sono aggiunti quelli allo stato solido (SSD) che hanno preso piede tanto nel settore professionale quanto in quello consumer. A ciò si deve aggiungere la diffusione di supporti esterni – di tipo sia HDD sia SSD – che possono essere spostati con molta facilità, ma che per questo motivo sono anche più esposti al rischio di danneggiamento. Cerchiamo quindi di fissare alcuni concetti chiave per districarci meglio tra le diverse casistiche nelle quali si può incorrere. A seguito di un evento che non permette di accedere ai dati possiamo distinguere tra un guasto che richiede un recupero software e uno che richiede un intervento di hardware o misto hardware e software.
Nel primo caso rientrano situazioni determinate da una corruzione del file system, dalla cancellazione dei dati eseguita per errore o volontariamente e dalla formattazione del supporto. In questo caso, ovvero quando il supporto hardware non ha subito alcun danno e funziona in modo corretto, il recupero dei dati è spesso possibile utilizzando strumenti software automatici specifici.
Nel secondo caso, quando il supporto di archiviazione ha subito un danneggiamento fisico – elettrico o meccanico – la



PARTI DI RICAMBIO

Il magazzino di Kroll Ontrack conta più di 10.000 pezzi che fanno capo a tutti i modelli e tipologie di dischi che sono stati commercializzati in passato e che sono presenti oggi sul mercato. Il magazzino è diviso in due sezioni: la prima è quella dove sono presenti i pezzi di ricambio di utilizzo più frequente, mentre la seconda costituisce un archivio storico di unità fuori commercio, ma ancora utilizzate.
Visto l'enorme investimento necessario a mantenere un archivio di questo tipo, Kroll Ontrack procede ad acquisti programmati tra le diverse sedi e in caso di necessità provvede a trasferire i pezzi di ricambio tra la sede che li ha in carico e quella dove sono necessari per una riparazione.

procedura di recupero è per forza di cose ben diversa. In questo caso i dati presenti sull'unità potrebbero essere intatti, ma poiché il supporto non funziona più in modo corretto questi potrebbero essere inaccessibili per il solo guasto hardware oppure potrebbero essersi anche corrotti per un malfunzionamento hardware.

HDD: DISCO DI TIPO MECCANICO

Il disco rigido è uno dei pochi componenti con parti meccaniche che ancora oggi è presente all'interno di un computer in ogni sua possibile forma: notebook portatile, desktop da scrivania, workstation o server. Come tutti i sistemi meccanici complessi che utilizzano parti in movimento, anche il disco rigido è soggetto a usura e guasti che ne possono compromettere il corretto funzionamento e l'utilizzo. Le parti meccaniche in movimento all'interno di un disco rigido sono: il motore di spin dei piattelli, i piattelli stessi (generalmente più di uno), il braccio porta testine e le testine, l'attuatore per il movimento e il posizionamento delle testine stesse e l'elettronica di controllo. Questi componenti sono assemblati in modo che i piattelli, rivestiti di un sottilissimo film con proprietà magnetiche e in rotazione attorno all'asse del motore principale, sono scanditi dalle testine che, viaggiando a bassissima distanza dai piattelli, procedono alla immagazzinare e recuperare le informazioni memorizzate sui piattelli stessi. Tutti questi componenti possono subire un guasto a causa di variazione o interruzione dell'alimentazione, rotture meccaniche, scariche elettrostatiche o problemi elettronici.

A dispetto dei possibili problemi che possono incorrere utilizzando parti meccaniche in movimento, i dischi rigidi classici hanno il grande vantaggio di offrire al tempo stesso sia le maggiori capacità di archiviazione per singola unità in valore assoluto, sia il miglior rapporto tra spazio di archiviazione e costo.

Prima di iniziare un intervento tecnico su un disco rigido è necessaria un'analisi accurata per determinare in modo preciso la causa del guasto o del problemi che ha reso inaccessibili i dati in esso contenuti. Solo una volta individuato il problema si avranno le informazioni necessarie per capire se è possibile ripristinare l'operatività del disco in modo da poter creare un'immagine completa delle informazioni contenute nel disco stesso.

Disco meccanico
Offre il miglior rapporto tra spazio e costo, così come le maggiori capacità

L'obiettivo di un intervento tecnico di recupero dati, infatti, non è mai quello di riparare il disco per poterlo usare come se il guasto non fosse mai avvenuto, ma è quello di riattivarlo per il tempo necessario a prelevare e mettere in sicurezza il suo contenuto. Una volta aperto, anche in camera bianca, un disco rigido riparato e richiuso non risponde più agli standard di funzionamento per i quali è stato progettato e secondo i quali è stato assemblato in fase di produzione.
Di seguito forniamo una casistica dei principali guasti nei quali possono incorrere i dischi rigidi meccanici. Il primo guasto che analizziamo è quello a carico della testina elettromagnetica, l'elemento che si occupa nella dinamica interna del disco di interpretare le variazioni magnetiche memorizzate sul piatto riportandole in linguaggio binario (lettura dati) o di magnetizzare porzioni microscopiche dello stesso nel processo di scrittura. I danni alla testina si dividono in elettrici e meccanici, con gravità e ripercussioni sul possibile recupero dati molto diverse. Nel primo caso, se la testina subisce un danno che impedisce la corretta lettura e scrittura dei dati dal punto di vista elettromagnetico non viene infatti intaccata fisicamente la superficie del disco, mentre nel secondo caso, quando a rompersi è il meccanismo di ritenzione della testina al di sopra del piatto le cose cambiano drasticamente.
In questo caso si possono determinarsi danni collaterali irrimediabili, come la rigatura diretta del piatto o la rottura di altri elementi di contorno. Le cause di danni di questo tipo sono molto diverse: nel primo caso si tratta di un guasto elettronico dovuto spesso a sbalzi di tensione che sebbene siano riconducibili all'elettronica di gestione finiscono per rovinare la testina stessa. Nel secondo caso il danno è spesso pregresso, come può esserlo un difetto di fabbricazione o uno stress del componente nel tempo e una conseguente rottura da usura. A questo può aggiungersi anche un danno dovuto a un trauma derivante da un colpo o da una caduta del dispositivo in funzionamento, ma anche spento.
Un contatto della testina sul piatto, detto crash è il danno più comune di tipo meccanico e anche quello dalle conseguenze più devastanti. Per immaginare il danno provocato da una testina che sbatte accidentalmente su

Una delle postazioni professionali di Kroll Ontrack. Si tratta di una camera bianca conforme agli standard ISO 14644-1 class 5 in grado di garantire la sicurezza di non danneggiare i supporti con particelle di polvere durante questa delicatissima fase di intervento.

uno dei piatti del disco basta immaginare che la superficie del disco ruota normalmente ad almeno 5.400 giri al minuto (notebook), con modelli da 7.200 giri o superiori presenti in tutti i sistemi desktop o nei notebook più veloci. Una testina ha dimensioni lillipuziane, con una larghezza inferiore a 100 nm e una larghezza di circa 30 nm e resta sollevata dai piatti del disco a un'altezza che può essere conteggiata in atomi. La distanza della testina è infatti nell'ordine di una decina di nm. Ecco un esempio esplicativo molto folkloristico, ma di sicuro impatto: immaginando che la testina sia grande quanto un aereo di linea e che la superficie terrestre rappresenti il piatto magnetico si può immaginare che l'aereo viaggerebbe a circa 1.000.000 di km/h a un'altezza dal suolo di pochi centimetri, mentre i passeggeri dovrebbero contare ogni singolo filo d'erba e non sbagliarne più di 10 in un territorio grande quanto la Lombardia.

Questo basta per immaginare quali danni possa fare sulla superficie del disco una testina che vi impatta in modo diretto asportando fisicamente lo strato magnetico nel quale sono contenute le informazioni. Altri possibili danni che possono presentarsi con un disco meccanico sono quelli imputabili al sistema di rotazione dei piattelli. A seguito di un colpo o di un urto particolarmente inteso, l'asse di rotazione del motore potrebbe disallinearsi con il resto della meccanica. Una variazione anche minima dell'asse di rotazione comporta infatti gravissimi problemi di lettura e scrittura del supporto, costringendo la testina magnetica a cercare di leggere dati dove in realtà si sovrappongono celle magnetiche differenti e scrivendo in posti che magari sono a cavallo tra più settori adiacenti.

Per procedere al recupero dei dati presenti sui piattelli – se non fisicamente rovinati – i tecnici devono rendere di nuovo operativa l'unità riparando il guasto elettronico, quello meccanico o un guasto combinato. Per fare questo può essere necessario sostituire l'elettronica, aprire fisicamente il disco per sostituire o ricalibrare le testine o, ancora, per riportare in asse il gruppo dei piatti. Si tratta di una riparazione complessa che richiede tempo, strumentazione professionale e una magazzino fornito dei pezzi di ricambio necessari.

RAID: PIÙ DISCHI RAGGRUPPATI

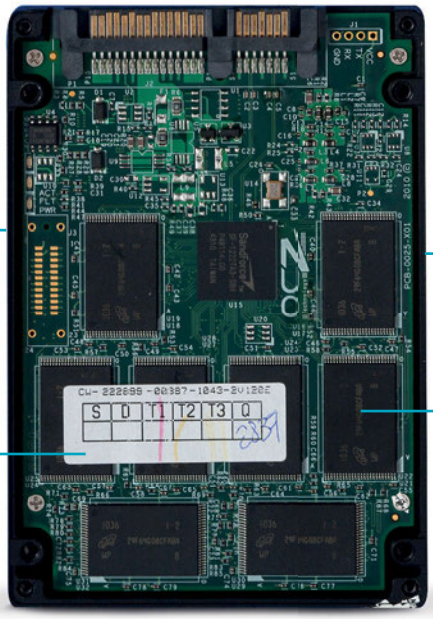
Se recuperare i dati da un singolo disco rigido è complicato, ma tutto sommato un'attività concettualmente semplice, non si può dire altrettanto per i sistemi Raid. Le complessità introdotte dai meccanismi di protezione Raid e dalla loro specifica implementazione sono molteplici: i sistemi Raid sono pensati per distribuire i dati su diverse unità aggiungendo codici di controllo, ma le informazioni nel singolo disco sono utili solo se correttamente allineate e ricostruite con tutte le altre facenti parte dello stesso set di dischi che costituiscono l'array Raid originale.

Inoltre, l'organizzazione dei dati sui diversi dischi che compongono l'array è diversa in funzione del tipo di protezione scelta (Raid 5, Raid 6, ecc), della versione del firmware del controller, ma anche di particolari configurazioni impostate sul sistema. A tutto ciò è necessario aggiungere anche che l'utilizzo di tecnologie proprietarie sviluppate dai produttori per migliorare l'efficienza di immagazzinamento dei dati, introducono un ulteriore grado di complessità al problema. Nelle soluzioni che prevedono la deduplicazione dei dati, ad esempio, la perdita di una piccolissima parte di dati può seriamente compromettere l'integrità di tutto il sistema.

Detto ciò è abbastanza intuitivo comprendere come il ripristino dei dati immagazzinati in un array Raid è molto più complicato rispetto alla ricostruzione di un disco rigido singolo. In questo caso non è sufficiente solo recuperare i dati grezzi, ma è necessario ricostruire in modo corretto tutti i livelli intermedi della struttura dati, compresi gli algoritmi propri del controller Raid utilizzato. Nei casi più gravi, il processo di ripristino di un array Raid può richiedere il recupero delle immagini dei singoli dischi che compongono l'array – anche quelle dei dischi non danneggiati – per poi simulare il comportamento dell'array stesso

DEDUPLICAZIONE

La deduplicazione è un processo in cui ogni elemento di un dato, soggetto a backup, è confrontato con un record dei dati che sono stati precedentemente archiviati per identificare una possibile ripetizione o ridondanza. Questo processo può avvenire prima o dopo che il dato è stato scritto nello sistema di storage dedicato al backup. Si parla di deduplicazione inline quanto le procedure viene eseguite in tempo reale, mentre il dato viene scritto sul disco di backup. Ma il processo di deduplicazione può avvenire dopo che i dati hanno subito il backup su disco e il processo di backup è terminato. In generale la deduplicazione in tempo reale impegna in modo intensivo la Cpu attraverso i suoi algoritmi che analizzano i dati in arrivo in modo da eliminare le duplicazioni prima che i dati finali siano scritti su disco.



in un ambiente virtualizzato e attraverso software progettati in modo apposito. Abbiamo introdotto il discorso relativo agli array Raid perché i concetti esposti fino a questo momento sono utili per comprendere la complessità di un recupero dati da eseguire su supporti di tipo SSD. Come vedremo, in questo caso più celle di memoria sono collegate tra loro in modo concettualmente simile a come avviene in un array Raid per creare il volume di archiviazione finale.

SSD E MEMORIE FLASH: DISCHI ALLO STATO SOLIDO

Nel mercato consumer più che in quello aziendale ed enterprise, le memorie flash si sono trasformate da nuova frontiera a soluzione standard. Pensiamo agli smartphone, alle macchine fotografiche digitali, ai computer portatili e a quelli desktop così come ai dischi portatili e alle chiavette Usb. Tutti noi possediamo almeno un dispositivo che utilizza una memoria allo stato solido. Queste memorie hanno il grande pregio di non avere parti meccaniche in movimento e per questo motivo è difficile che si guastino a seguito di una caduta, anche se non si può dire altrettanto dei dispositivi che le contengono. Se il guasto meccanico è quindi pressoché impossibile, non possiamo dire altrettanto per quello elettronico. Ogni tanto, soprattutto quando si utilizzano prodotti molto economici (ad esempio chiavette Usb), capita che un supporto flash smetta di funzionare o che si danneggi a seguito di uno sbalzo di tensione.

Dischi allo stato solido
Sono veloci e resistenti agli urti, ma soggetti a possibili guasti elettronici

Come per i dischi meccanici ci sono quindi vantaggi e svantaggi. Da un alto l'industria segue standard ben codificati nella produzione di memorie Nand, ma questa è solo metà della storia perché la vera complessità dei sistemi basati su tecnologia flash deriva da due elementi critici che spesso non sono valutati in modo adeguato. Il primo è che i chip di memoria sono inutili se non accoppiati con un controller specializzato e dotato di un firmware sviluppato in modo apposito. Se il chip di controllo può essere un componente ampiamente utilizzato e conosciuto, altrettanto non possiamo dire per il firmware che molto spesso è sviluppato e aggiornato internamente dall'azienda produttrice. Lo scopo di questo sviluppo non standard è dettato anche dalla necessità di implementare tecnologie studiate per migliorare la durabilità delle memorie flash, la consistenza dei dati o le prestazioni per battere la concorrenza. Proprio i rapidi aggiornamenti caratteristici di questo mercato determinano la difficoltà di ricostruire gli algoritmi con i quali i dati sono archiviati all'interno delle memorie Nand. La difficoltà principale nel recupero di dati da un'unità o da un dispositivo che utilizza una memoria flash è nella maggior parte dei casi di tipo logico e riguarda l'organizzazione dei dati; a volte però è possibile che siano proprio le celle di memoria Nand ad essere danneggiate e in questo caso il recupero del loro contenuto può essere impossibile come accade quando viene danneggiato il film magnetico di un disco rigido.

Il processo di recupero è comunque concettualmente simile a quanto già descritto, ma diverso dal punto di vista pratico: si cerca di ripristinare il funzionamento anche parziale del dispositivo o si procede a dissaldare i chip di memoria per estrarre i dati in essi contenuti mediante uno strumento apposito che ne permetta la lettura. Come abbiamo accennato, i dischi SSD sono realizzati da più chip di memoria collegati tra loro attraverso il controller. Nel caso di queste unità quindi si procede in modo simile a quanto descritto per un array Raid: si recuperano le immagini dei dati presenti in ogni singolo chip di memoria Nand e si tenta di simulare il funzionamento del controller in ambiente virtualizzato con strumenti software specifici.

GUASTI SOFTWARE

Fino ad ora abbiamo parlato esclusivamente di guasti hardware, ma questa è solo una parte del problema. Uno guasto software, compreso l'errore umano, è più probabile di uno hardware e non è detto che a seguito di un guasto hardware non si riscontri anche un conseguente problema di consistenza dei dati da un punto di vista software.

Quando si verifica un guasto all'hardware di un dispositivo, questo può comportarsi in modo anomalo dando origine a un conseguente guasto software che si somma a quello hardware che l'ha generato.

Se il problema è solo di tipo software, l'intervento di recupero è relativamente più semplice in quanto il supporto di archiviazione funziona in modo corretto. Spesso è sufficiente utilizzare tool specifici – ne esistono anche di pubblico dominio – che eseguono la scansione del file system con lo scopo di correggere gli errori software per recuperare i dati non leggibili. Anche in questo caso rimane sempre valida la regola che un intervento sbagliato piattaforma compromettere in modo definitivo i dati.

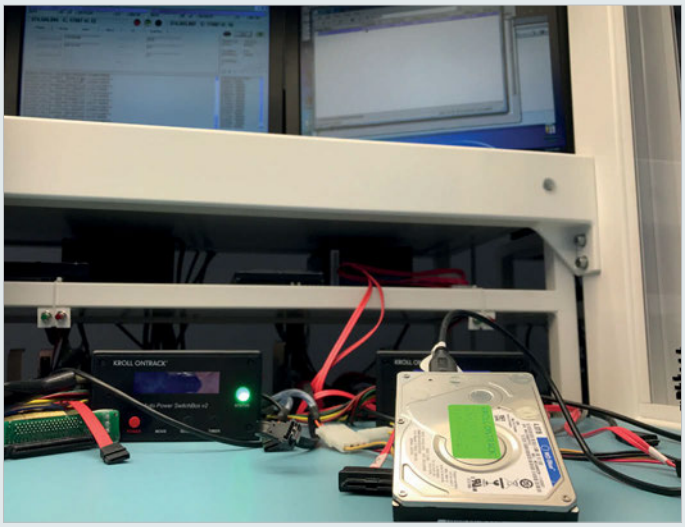
LA PROVA DI KROLL ONTRACK

La nostra prova reale su un disco danneggiato di proposito: tutte le fasi del processo di recupero dati in camera bianca su un disco esterno meccanico.

Per una prova sul campo di come è possibile tentare il recupero dati da un supporto danneggiato ci siamo affidati al servizio offerto da **Kroll Ontrack**. L'azienda ci ha permesso di visitare le proprie strutture – compreso il laboratorio con le camere bianche – sia di seguire passo passo lo svolgersi delle operazioni eseguite sul disco di test da noi fornito.
Poiché l'intenzione della nostra prova era di verificare sul campo cosa e come fosse possibile recuperare da un disco danneggiato, abbiamo deciso di simulare il danneggiamento di un'unità di archiviazione e di sottoporre quest'ultimo a un servizio di recupero professionale. Il nostro supporto – un disco Usb 3.0 esterno da 4 Tbyte e tecnologia meccanica – è stato danneggiato di proposito simulando una caduta. Nello specifico abbiamo messo il disco privo di protezioni aggiuntive all'interno di un borsa che potrebbe essere usata comunemente per i tragitti casa-ufficio da moltissimi utenti; abbiamo quindi simulato la caduta della borsa lungo una rampa di scale come potrebbe capitare a una qualunque persona che perde l'equilibrio e tenta di aggrapparsi a un sostegno lasciando andare ciò che ha in mano. Con nostra grande sorpresa è stata sufficiente una singola cauta per rendere il disco inutilizzabile o quantomeno per precludere l'accesso ai dati archiviati sul disco stesso. Il primo passo in assoluto da compiere prima di intraprendere una procedura di recupero dati è quella che consiste nel prendere contatto con il fornitore del servizio – in questo caso Kroll Ontrack – descrivere la problematica e richiedere un preventivo. Un volta espletate le fasi che riguardano una prima diagnosi in base a quanto descritto dal cliente e l'accettazione del preventivo relativo alla lavorazione, la fase successiva consiste nell'inviare al servizio di recupero dati il supporto danneggiato. Quando il supporto raggiunge la propria destinazione ha inizio la lavorazione vera e propria da parte del team tecnico.

1 I RESTRAZIONE E ANONIMATO

Il primo passaggio prevede la registrazione del supporto all'interno del sistema informatico di tracciamento delle lavorazioni; il supporto è quindi assegnato per il recupero dati e riposto in un bin (una vaschetta antistatica) identificato da un ID univoco. Nel caso specifico di Kroll Ontrack, a seconda dell'urgenza di lavorazione (scelta dal cliente in fase di definizione del servizio sulla base delle proprie esigenze) i bin utilizzano un codice colore differente in modo da consentire allo staff tecnico di riconoscere visivamente gli interventi prioritari (bin rosso) da quelli standard (bin blu). La fase di registrazione del disco implica anche la catalogazione di tutte le eventuali componenti inviate dal cliente e che accompagnano l'hard disk stesso. Ad esempio, box esterni e/o adattatori vengono anch'essi etichettati con il numero della lavorazione. Questa procedura permette di organizzare al meglio e di rendere più efficiente la logistica di tutto ciò che viene ricevuto.

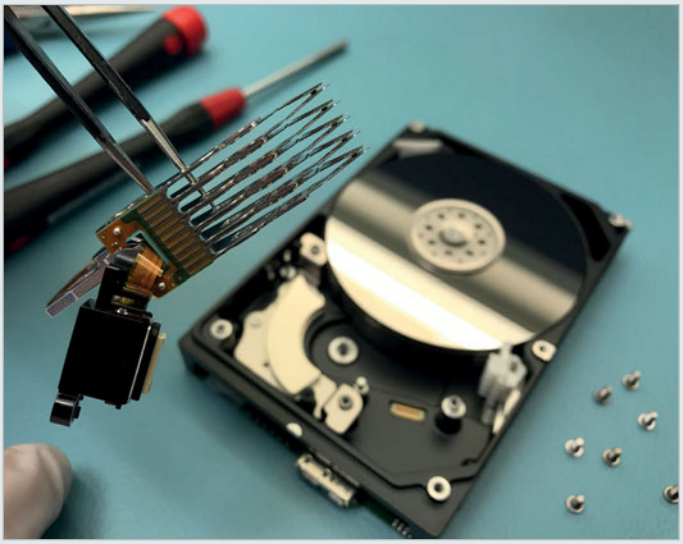


2 | FASE DI DIAGNOSI

Il disco è stato sottoposto ad una preliminare fase di analisi attraverso specifici tool proprietari. Tale fase ha l'obiettivo di verificare la funzionalità del dispositivo e di identificare eventuali problematiche. In questo specifico caso, è stato possibile attraverso nostri strumenti riconoscere fisicamente l'hard disk tuttavia non è stato possibile avere accesso ai dati.
I sistemi di diagnostica utilizzati da Kroll Ontrack prevedono l'impiego di una interfaccia intelligente: qualora venga rilevato un problema grave al disco nei primi istanti di accensione, il sistema provvede a tagliare l'alimentazione in modo da evitare che le testine impattino sui piattelli del disco e rovinino in modo irreversibile la superficie magnetica sulla quale sono immagazzinate le informazioni da recuperare. Questa è una fase delicata e che richiede molta esperienza da parte dell'operatore tecnico che procede alla diagnosi.

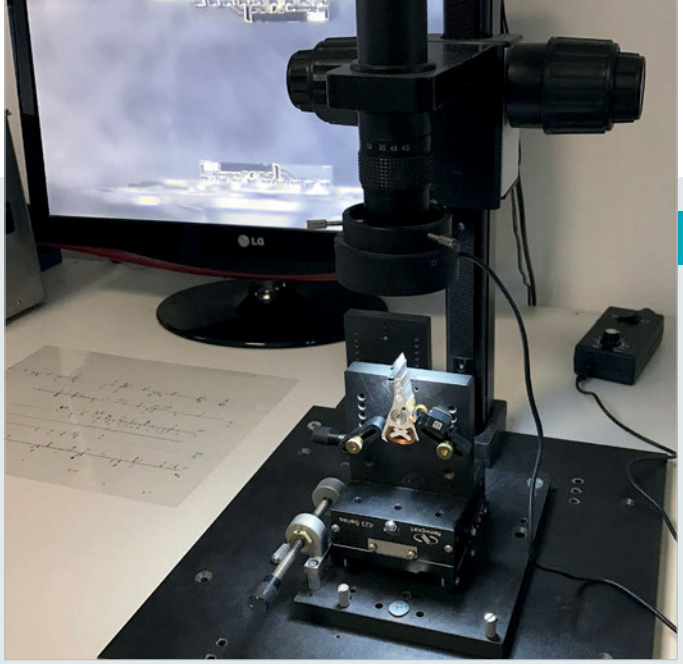
3 | APERTURA DEL DISCO

Verificata l'impossibilità di aver accesso alla lettura dei dati contenuti nell'hard disk, da procedura abbiamo provveduto all'apertura del disco in camera bianca. La camera bianca professionale di Kroll Ontrack, le cui postazioni di lavoro seguono gli standard ISO 14644-1 class 5, garantisce grazie anche alle competenze dei nostri esperti l'assoluta sicurezza di questa delicatissima fase, è fondamentale infatti agire con estrema abilità e proteggere la superficie magnetica dei piatti del disco dall'eventuale deposito di pulviscolo e altre particelle contaminanti che potrebbero determinare un serio rischio per la buona riuscita dell'intervento.
Lo scopo dell'operazione non è quella di riparare in modo definitivo, ma di renderlo operativo per il tempo sufficiente a estrarre e mettere in sicurezza i dati – in formato grezzo – in esso contenuti.



4 | INTERVENTO

Nel caso in esame, una volta aperto il disco, i nostri esperti hanno rimosso il blocco testine per sottoporlo ad una successiva ispezione visiva tramite l'impiego di un microscopio dedicato per verificare la presenza di danni non osservabili a occhio nudo. L'urto al quale abbiamo sottoposto il disco in modo volontario ha disallineato le testine rispetto alla loro posizione originale. Per questo motivo, anche se il disco è stato correttamente riconosciuto dal sistema di diagnostica al quale è stato collegato, le testine di lettura non sono state in grado di agganciare le tracce magnetiche presenti sui piattelli e di leggere in modo corretto i dati in essi contenuti.
Per ripristinare il funzionamento del disco è stato quindi necessario smontare il braccio delle testine per procedere a una loro analisi approfondita prima di procedere a una nuova fase di allineamento con i piattelli del disco.

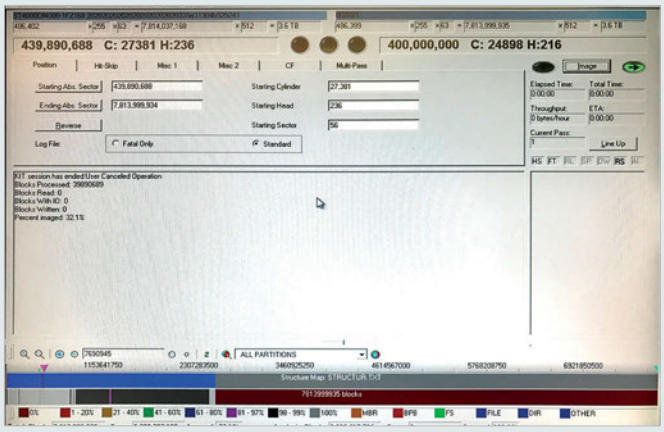


5 | CONTROLLO

Le testine, una volta smontate dal disco originale, sono state posizionate al microscopio per un'ispezione visiva approfondita. L'immagine ingrandita del gruppo testine è inviata ad un monitor che permette ai tecnici un'osservazione più accurata e precisa. L'obiettivo consiste nell'individuare eventuali anomalie non visibili ad occhio nudo, ad esempio potenziali danni oppure la contaminazione delle testine causata da minuscole particelle di materiale rimosso dalla superficie magnetica a seguito di un accidentale contatto testina-disco. In caso di danneggiamento, le testine sono momentaneamente sostituite con quelle di un disco identico presente nel magazzino delle parti di ricambio. Questa fase mostra la complessità dell'intervento e la necessità di avere a disposizione strumentazione ed esperienza che solo un servizio di tipo professionale è in grado di garantire.

6 | RIASSEMBLAGGIO

Non avendo riscontrato anomalie o danni a carico delle testine originali del disco danneggiato, i tecnici hanno proceduto al loro ripristino. Dopo aver sottoposto le testine ad un ciclo di pulizia ed aver proceduto a verifica strumentale degli altri componenti, l'hard disk è stato riassemblato utilizzando tutti i pezzi originali. Sempre in relazione alle testine, è stato verificato e corretto anche il loro allineamento, in modo da permettere la corretta lettura dei dati contenuti sui piattelli magnetici. Anche questa fase è stata eseguita in camera bianca in modo da essere sicuri che all'interno del disco, una volta richiuso, non fossero presenti particelle di polvere che potessero danneggiare le testine e i piattelli. Il disco così riassemblato è stato utilizzato solo per l'estrazione dei dati grezzi che sono stati salvati sui server di lavorazione di Kroll Ontrack per la successiva fase di recupero.



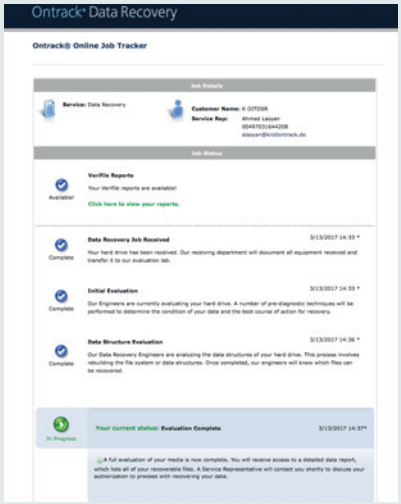
7 | RECUPERO DEI DATI

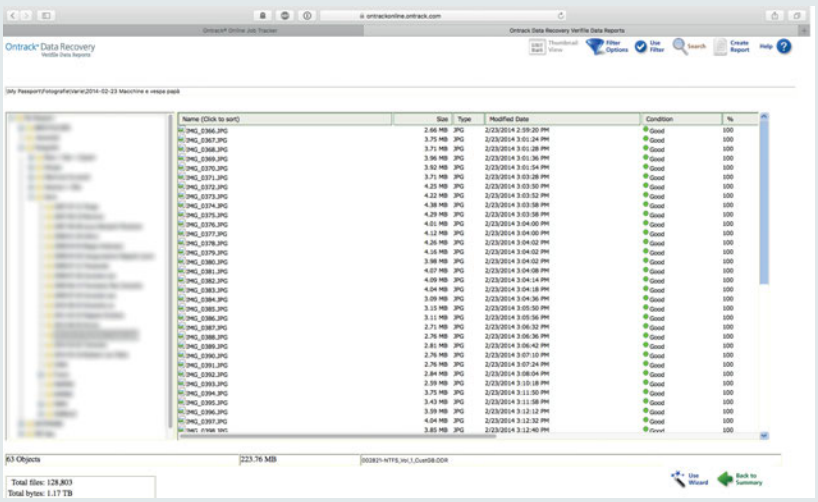
L'hard disk riassemblato è stato successivamente collegato ai nostri sistemi per eseguire un'immagine raw del suo contenuto, il salvataggio è stato fatto su uno dei nostri server dedicati. L'immagine "grezza" è stata quindi presa in carico dal team tecnico del Lab. In questa fase i tecnici hanno verificato l'integrità dei dati, corretto eventuali errori riscontrati per poi dedicarsi alla ricostruzione della struttura logica dei singoli file (nel formato comunemente utilizzato dell'utente) con l'aiuto di strumenti software proprietari. Nei casi più semplici il processo avviene in modo automatizzato, ma nei casi più gravi può essere richiesto l'intervento tecnico di personale specializzato per risalire a complesse strutture di dati – volumi Raid, macchine virtuali, ecc – difficili da ricostruire con il solo utilizzo di strumenti software automatici.

8 | DATI AL SICURO

Conclusa l'attività del Lab, i dati - ora disponibili in forma classica - sono stati copiati in formato crittografato su un disco esterno di backup con interfaccia Usb 3.0 e pronto per essere consegnato al cliente. La crittografia applicata permette di innalzare il livello di sicurezza sui file, proteggendoli fino a quando il supporto non sarà stato consegnato nelle mani del cliente. La password viene inviata al cliente separatamente dalla spedizione insieme con le istruzioni per l'accesso ai dati stessi. Come si vede sul disco non compare mai il nome del cliente in quanto in ogni fase del recupero il supporto è identificato solo dal codice di lavorazione.

9 | IL REPORT DELL'INTERAZIONE CON IL CLIENTE





Tra la fase 7 e 8, all'utente viene fornita la possibilità – in base al servizio richiesto – di verificare una valutazione del recupero dati possibile attraverso la piattaforma online di Kroll Ontrack. Accedendo al portale con le credenziali fornite dall'azienda è possibile osservare la struttura delle directory e verificare la bontà del recupero di ogni file attraverso una grafica molto semplice: bollino verde, bollino giallo e bollino rosso a fianco di ogni singolo file estratto durante il recupero dei dati. Il bollino verde viene assegnato quando i controlli di validità del file sono stati superati al 100%. Il bollino giallo viene assegnato quando il file è stato recuperato in modo parziale, ma le informazioni di controllo sono sufficienti per tentare un recupero completo del file. Il bollino rosso viene assegnato quando le informazioni relative a un file sono parziali e non sufficienti per recuperare in modo completo il file; in questo caso il recupero è impossibile oppure è possibile tentare un recupero parziale dello stesso, ma ovviamente con una perdita di informazioni. Se il cliente è soddisfatto, si procede con il recupero finale e con l'invio del supporto contenente i dati.

10 | I DATI RECUPERATI

Durante tutta al fase di recupero, infatti, il nome del cliente non viene mai associato al particolare disco in lavorazione, così come non viene mai aperto in modo effettivo alcun file.
Il cliente riceve il supporto originale e il disco con i dati recuperati. Kroll Ontrack consiglia di procedere appena possibile a una copia in chiaro dei dati inviati in modo da metterli in sicurezza. L'immagine dei dati rimane per qualche giorno sui server interni di Kroll Ontrack così da poter rispondere ad ulteriori esigenze del cliente; il team di supporto commerciale dell'azienda rimane in contatto con il cliente stesso per tutto il tempo di lavorazione. Se non ci sono problemi i dati sono cancellati dai server. Il costo dell'intervento è variabile e dipende dal tipo di guasto e dall'urgenza del recupero. Una volta accettato il preventivo proposto in fase iniziale, quello è l'effettivo costo a carico del cliente e non vi saranno modifiche anche se durante la lavorazione si presentasse la necessità di interventi più consistenti a quelli preventivati.