ANALISI DEL DISCO FISSO DI UN SISTEMA DI VIDEOSORVEGLIANZA: UN ESEMPIO DI *REVERSE ENGINEERING*

di Paolo Reale

Probabilmente molti ricordano il caso della bomba nella scuola di Brindisi, a maggio 2012, che è stato risolto grazie alle registrazioni video di alcune telecamere di sicurezza: in effetti, il numero di sistemi di videosorveglianza in uso, per ragioni di sicurezza e per combattere la criminalità, è cresciuto notevolmente negli ultimi anni, e anche se è difficile fare una stima (non essendo necessarie particolari autorizzazioni per l'installazione, non sono disponibili numeri precisi), secondo alcune valutazioni in Italia ci sarebbero circa due milioni di telecamere.

La tecnologia utilizzata per la registrazione video da queste telecamere, in passato basata su memorizzazione su nastro, ormai da anni utilizza il formato digitale, mediante *hard disk* o dispositivi a stato solido. Nel corso del tempo si sono sovrapposte molte soluzioni tecniche, per cui quando si parla di "Videoregistratore Digitale" (o DVR, *Digital Video Recorder*) in realtà si parla di una variegata eterogeneità di apparati, che utilizzano sistemi operativi e tecnologie di compressione differenti. Se il DVR è funzionante, di solito non sussistono particolari problemi nel recupero ed utilizzo dei dati registrati, generalmente tramite i *software* proprietari per la copia e la relativa riproduzione.

Non è raro però il caso in cui il dispositivo DVR, che per qualche ragione è di interesse in un procedimento giudiziario, è danneggiato, oppure la struttura memorizzata (ad es. il *file system*) è compromessa, o volontariamente cancellata. In questi casi, solitamente, ci si deve rivolgere al produttore del dispositivo.
Se anche questa soluzione non è percorribile, esiste una sola alternativa: l'attività di *reverse engineering*, ovvero il processo di ricostruire il funzionamento di un meccanismo– in questo caso informatico – **partendo dall'analisi del suo risultato**. Cercando di semplificare, l'attività di *reverse engineering* consiste nell'utilizzo di un sistema identico (l'originale stesso, se possibile, o un altro perfettamente uguale), sul quale effettuare delle simulazioni sperimentali ben determinate, osservando quello che il sistema produce e da qui comprendere come e dove vengono memorizzate le informazioni.
In questa sede cercheremo di analizzare come sia possibile affrontare questa attività per uno specifico modello, l'HS-DVR 163, su cui è stata portata a termine con successo detta attività di ricostruzione: nel caso esaminato il disco era risultato non più leggibile dal sistema, come se fosse stato inizializzato, pur presentando al suo interno dati per tutta la sua capacità. I risultati qui presentati non possono essere validi per tutti gli altri modelli di DVR, ovviamente, ma l'approccio metodologico adottato sì, così come è vero che il funzionamento di questi apparati utilizza logiche tra loro simili, ovvero vengono utilizzate (da un punto di vista logico) strutture dati e meccanismi analoghi.

In primo luogo va precisato che, specie per gli apparati meno recenti, il supporto di memorizzazione (tipicamente un disco fisso come quelli che vengono utilizzati nei normali PC) deve assolvere la stessa funzione di un nastro, ovvero la registrazione continua di una serie di fotogrammi provenienti dalle telecamere: per detta ragione viene spesso adottata in questi dispositivi una modalità di scrittura sul disco ad accesso diretto, nel senso che non viene demandata ad un *file system* la memorizzazione dei dati. Questa soluzione, se dal punto di vista del produttore consente di ottimizzare (e velocizzare) le operazioni di lettura/scrittura sul disco, rende ancora più arduo il compito per chi deve poi interpretare le informazioni presenti. Innanzitutto perché, a seconda del microprocessore utilizzato, i dati possono essere gestiti utilizzando la modalità *little endian* o *big endian*: questo fa sì che sul disco i dati possano trovarsi rappresentati sia nella modalità "abituale" in cui il *byte* più significativo precede quello meno significativo, sia in quella contraria.

Nel caso del dispositivo in esame, i dati sono salvati in formato *little endian* (il *byte* meno significativo precede l'altro). Per analizzare il disco utilizzando strumenti *standard* è stato quindi necessario procedere ad un'operazione di "*swap*" dei *byte*, in modo da riportare il formato dei dati con il *byte* più significativo per primo. Grazie a questa operazione diventa banale il recupero di tutti fotogrammi presenti nel disco: utilizzando un qualunque programma di recupero dati (*carving*) che si basa sui "*magic numbers*" è possibile riconoscere i codici di inizio e fine delle immagini jpg e recuperarle integralmente. Nel caso del dispositivo in esame, in base alle caratteristiche note dal manuale, la registrazione viene effettuata nel formato M-JPEG (*Motion* JPEG), che prevede appunto la memorizzazione di ogni singolo fotogramma in formato JPG, senza compressione tra i fotogrammi (*inter-frame*).
Fin qui l'analisi non si rivela particolarmente complessa. Il problema, a questo punto, è la correlazione del fotogramma alla sua informazione temporale. Nella fattispecie, infatti, i fotogrammi non contengono alcuna indicazione sovraimpressa, né metadati (EXIF) riportanti alcuna informazione.

❶ *Ambiente simulato*

A questo punto necessariamente si deve ricorrere al "*reverse engineering*": occorre recuperare un modello identico dell'apparato DVR oggetto di analisi, alcuni dischi fissi, opportunamente "azzerati" di tutti i loro contenuti (ovvero riempiti di "zeri"), una sorgente di segnale video per simulare le telecamere e quindi poterne registrare il segnale sui dischi di prova.
In questo modo è possibile rilevare come il sistema DVR memorizzi i dati sul disco fisso: al termine delle prove predefinite, il di-

sco contenente i dati prodotti dal DVR può essere letto tramite un PC al fine di individuare i contenuti memorizzati dal sistema DVR, e da qui cercare di comprendere il significato funzionale.

Tra le prove effettuate, *in primis* è stata verificata l'operazione di inizializzazione operata dal DVR sui dischi fissi inseriti, che ha consentito già di giungere ad un primo risultato: individuare la codifica utilizzata per la rappresentazione della data e ora. Successivamente, tramite la ripetizione di brevi registrazioni, si è cercato di individuare, sul disco, le zone utilizzate e le ulteriori informazioni scritte dal sistema DVR.
È chiaro che un'attività di *reverse engineering* di questo tipo è molto dispendiosa in termini di tempo, in quanto non solo richiede l'esecuzione di tutta una serie di prove fisiche, e delle successive letture ed acquisizione dei dati, ma soprattutto necessita di una complicata fase di analisi, destinata innanzitutto all'individuazione delle informazioni utili e quindi alla loro comprensione come logica di funzionamento. Occorre un po' di pazienza e di intuito.
In foto un *setup* predisposto per questo tipo di analisi.

❷ Inizializzazione del disco fisso

Quando in questo DVR si inserisce un disco "non riconosciuto" (nuovo, o formattato con altri *file system*) questo viene "inizializzato": vengono scritte una serie di informazioni destinate a rendere utilizzabile il disco e quindi poterci registrare i segnali provenienti dalle telecamere. In particolare, con certezza, viene inserita la data e l'ora corrente. La data/ora di inizio e di fine registrazione vengono inserite nel primo settore del disco. **Questo settore costituisce di fatto una tabella contenente alcuni dati di riepilogo e di indirizzamento, e per questa ragione la definiremo "*Master Table*" nel seguito**. Una tabella di questo tipo è generalmente sempre presente in queste tipologie di DVR, anche differenti dal modello in esame. È certamente il punto di partenza per capire il funzionamento del sistema.

Nella tabella qui riportata sono indicate le posizioni delle informazioni temporali, e nell'immagine la rappresentazione tramite visualizzazione in esadecimale dei dati dalla *master table*. Ogni dato è espresso sotto forma di singolo *byte*, ovvero l'anno è codificato su un *byte*, in cui il valore '00' corrisponde all'anno 2000, e così via.

Posizione	Dato	Significato	Posizione	Dato	Significato
0x28	Anno (00=2000)	Data e ora di inizio registrazione	0x30	Anno (00=2000)	Data e ora di fine registrazione
0x29	Mese		0x31	Mese	
0x2A	Giorno		0x32	Giorno	
0x2B	Giorno della sett.	1=dom,..,7=sab	0x33	Giorno della sett.	1=dom,..,7=sab
0x2C	Ore		0x34	Ore	
0x2D	Minuti		0x35	Minuti	
0x2E	Secondi		0x36	Secondi	

❸ Test con registrazione video

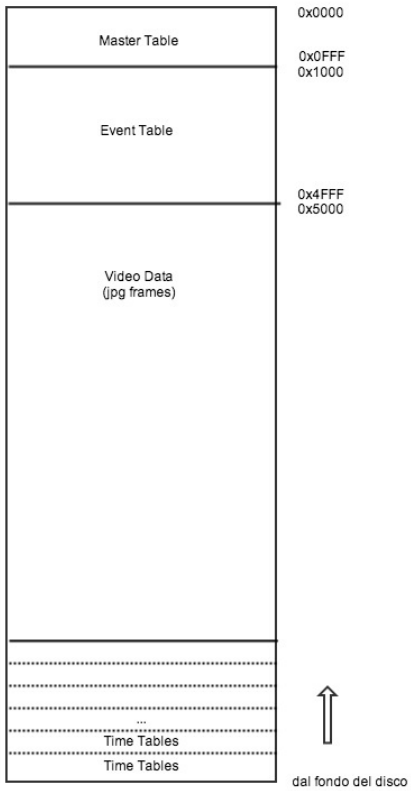
Una volta individuato il formato di scrittura di data e ora, tramite ulteriori prove di registrazione, è risultato possibile verificare la presenza delle altre "strutture dati" fondamentali, rappresentate in figura e descritte di seguito.

a) Master table

Risulta di interesse notare come la *Master Table* sia oggetto di continui aggiornamenti durante il funzionamento del dispositivo: le locazioni di memoria relative alla data di inizio registrazione vengono aggiornate quando viene effettivamente registrato qualcosa sul DVR.

b) Tabella degli eventi

La zona di memoria 0x1000-0x4FFF costituisce la rappresentazione codificata della "tabella degli eventi" o "*event table*". Gli eventi sono tipicamente, in questi sistemi, le rilevazioni di "*motion detection*" e altro ancora in base a quanto previsto dall'apparato.
Ogni elemento della tabella appare composto da 16 *bytes*, all'interno dei quali sono presenti diverse informazioni: nella figura della pagina successiva sono indicate le posizioni delle informazioni di interesse, ovvero dei *timestamp*.



È possibile anche verificare che questa tabella è proprio quella che viene visualizzata dall'utente tramite la funzione di sistema "*event list*" durante il normale utilizzo dell'apparato.
Nei *test* effettuati è stato possibile notare come questa tabella viene scritta in modo incrementale durante il funzionamento, e al termine della memoria predefinita il ciclo ricomincia (sovrascrivendo le precedenti informazioni) in modo da mantene-

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
#telecamera								anno	mese	giorno	Giorno della settimana	ore	minuti	secondi	00

Tabella degli eventi: singolo *record*

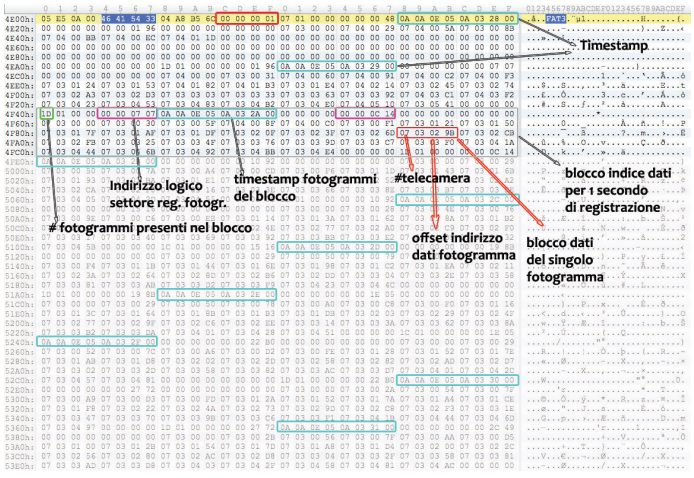
re sempre quella dimensione di tabella, che quindi consente la memorizzazione di un massimo di 1024 eventi.

c) *Zona dati video*

A partire dall'indirizzo 0x5000 compaiono i "*magic numbers*" relativi ai *file* immagine di tipo JPG. Le immagini sono memorizzate una di seguito all'altra, a partire dal primo *byte* del settore successivo. Infatti, in un disco fisso, il settore è l'unità minima che può essere memorizzata durante il ciclo di scrittura. Questa soluzione, oltre che più semplice, consente soprattutto di poter "indirizzare" ogni immagine utilizzando l'indirizzo logico.
Si ricorda che l'indirizzo logico del settore corrisponde all'indirizzo fisico diviso per 512 (decimale, oppure 200h esadecimale). Per fare un esempio concreto, la prima immagine JPG si trova all'indirizzo fisico 0x5000, che corrisponde all'indirizzo logico 0x28 (5000 hex = 20.480 in decimale, diviso per 512 fa 40, ovvero 0x28). Si dovrebbe quindi già intuire il vantaggio di questa scelta, che consente di "indirizzare" i dati sul disco "risparmiando" *byte*, ovvero rendendo più compatte e brevi le tabelle contenenti i dati di indirizzamento.

d) *Tabella dei tempi*

La "tabella dei tempi", qui battezzata indifferentemente come "*time table*" o "*time list*", come presente nel menù di sistema del DVR, si trova nella parte finale del disco. Tale tabella consente di poter visionare in *playback* (visualizzazione) i segmenti video registrati in quegli intervalli temporali.
Questa tabella, necessariamente, deve tracciare le informazioni relative all'associazione tra i singoli fotogrammi memorizzati sul disco e l'istante temporale a cui si riferiscono, in modo da consentire al sistema di poterli rintracciare e visualizzare.
La struttura delle tabelle dei tempi è caratterizzata da un codice testuale "FAT3" (che potrebbe essere l'acronimo di *File Allocation Table*, ovvero tabella di allocazione dei *file*) e di numerose altre informazioni. Questa struttura appare "ripetuta" (come struttura, e non come contenuti) in blocchi di dimensione fissa, esattamente 1536 *bytes* (600h in esadecimale).



Struttura della tabella dei tempi

Ogni struttura da 1536 *bytes* è una vera e propria tabella: certamente è possibile rilevare numerosi *timestamp*, oltre ad altre informazioni. Queste tabelle vengono scritte sul disco partendo dal fondo del disco stesso e procedendo a ritroso. In altre parole, la parte terminale del disco appare come una sequenza di queste tabelle, ognuna strutturata nello stesso modo, e scritte in sequenza inversa (dal fondo).
L'immagine prima riportata è un esempio estratto della prima *time table*, che si trova nell'ultima porzione del disco, ovvero "in fondo" al disco di prova utilizzato. Complessivamente la struttura individuata contiene 10 *timestamp* relativi a 10 secondi consecutivi. La *timetable* successiva (come già detto collocata nella memoria in posizione antecedente a questa) prosegue con i 10 secondi successivi. Al fine di discriminare la sequenza delle tabelle, è presente un "contatore" che viene incrementato ad ogni tabella successiva. Nell'esempio, detto indicatore è visibile nel *box* rosso (prima riga della figura) col valore di "01".
Per ogni secondo di registrazione è possibile identificare, a sua volta, una precisa rappresentazione dei dati. Nell'immagine precedente, è stato evidenziato in grigio un blocco dati relativo ad un secondo, per poterlo "dissezionare" nei suoi componenti elementari.

Il primo *byte* (*box* verde) rappresenta il numero di fotogrammi memorizzati per quel secondo di registrazione: nell'esempio 1D è la codifica esadecimale di 29, quindi quel blocco contiene le informazioni relative a 29 fotogrammi memorizzati in quel secondo. La struttura è pensata per poter contenere fino ad un massimo di 30 fotogrammi ogni secondo, massimo numero di fotogrammi al secondo supportati dal DVR esaminato.
Tra l'indicatore del numero fotogrammi e il timestamp di questo blocco, sono evidenziati in figura, in un riquadro fucsia, 4 *bytes* che identifichiamo come ***indirizzo_base*** del settore del disco in cui sono registrate le immagini JPG. Ricordiamo che l'indirizzo fisico può essere ricavato dall'indirizzo logico moltiplicando per 512. Il riquadro fucsia successivo, dopo il *timestamp*, è l'indirizzo base del settore del disco contenente i fotogrammi relativi ai 10 secondi successivi di registrazione.
Dopo questi 4 *bytes*, seguono 8 *byte* a zero, e dal successivo si possono identificare 30 strutture identiche di 4 *byte* ciascuna, che costituiscono l'indirizzamento del singolo fotogramma. Ovviamente nell'esempio indicato l'ultimo gruppo di 4 *bytes* sarà necessariamente a zero in quanto sappiamo che questo blocco contiene 29 fotogrammi. A titolo di esempio è stata evidenziata una di queste strutture in colore rosso. Il primo *byte* individua il numero del canale di ingresso, ovvero della telecamera, a cui si riferisce il fotogramma, il secondo *byte* contiene i parametri di configurazione relativi al fotogramma, i restanti 2 *bytes* costituiscono l'***offset*** per indirizzare il fotogramma in questione, tramite la formula: ***indirizzo_base+offset***.
Per quanto possa apparire complessa, questa analisi è stata possibile grazie al fatto che le strutture dati sopra descritte, per quanto differenti da un modello all'altro, sono – da un punto di vista logico – sempre presenti nei sistemi DVR. In conclusione, per chi deve eventualmente recuperare dati da questo stesso modello di DVR, può risparmiarsi tanto tempo prezioso grazie all'analisi qui esposta. Nel caso invece sia necessario realizzare un'attività analoga anche su altre tipologie di DVR, l'impostazione qui presentata rimane valida tecnicamente e logicamente. ©