Slack space e come si recuperano i dati all'interno

Lo slack space è quella porzione di cluster che originariamente conteneva dati di un file ora cancellato e che a seguito della scrittura di un nuovo file non è stato sovrascritto (in quanto l'ultimo blocco del nuovo non va a coprire l'intera dimensione del cluster).
I dati memorizzati all'interno dello slack space potrebbero essere usati per recuperare password e altri dati di accesso, parti di file, comunicazioni (ad esempio i messaggi istantanei) e molte altre tracce che potrebbero portare a informazioni interessanti. Tramite l'acquisizione fisica (bit per bit) sarà possibile recuperare lo slack space (l'acquisizione logica non lo permette), e sarà possibile visualizzare tali informazioni come sequenze di bit "non coerenti" con il resto del cluster allocato per un altro file.

Quali informazioni troviamo sul tabulato telefonico?

- Il numero di telefono del mittente/chiamante;
- Il numero di telefono del destinatario/chiamato;
- Data ed ora (secondi compresi) dell'inizio della conversazione o dell'invio del messaggio;
- Durata della conversazione (zero se trattasi di Sms o di chiamate perse);
- Tipo di evento (chiamata, chiamata persa, Sms).
- Bts agganciata durante la chiamata che permette di capire in quale cella telefonica, ovvero zona geografica, era localizzato l'interlocutore;
- Codice Imei del terminale mobile (cioè dello smartphone o del telefono cellulare utilizzato);
- Codice Iccid della scheda Sim utilizzata

Il tabulato telefonico non contiene i contenuti della comunicazione (registrazione della chiamata, contenuto del SMS...), impedendo così di utilizzarlo per comprovare la veridicità di un SMS.
Grazie alle informazioni sul tabulato telefonico sarà possibile effettuare una geolocalizzazione approssimativa di un dispositivo mobile, ponendo le BTS su una mappa, tracciandone le linee di handover (linee equidistanti tra due BTS secondo le quali il dispositivo mobile di scollega dall'antenna di provenienza per via del peggioramento di segnale per collegarsi ad un'altra antenna). Lo studio degli handover non fornisce tuttavia elemento probatorio sufficiente, infatti bisognerà cercare di comprovare la geolocalizzazione tramite tabulati con ulteriori elementi (come il collegamento a reti wifi libere, l'emissione di scontrini, il pagamento di pedaggi autostradali...)

Differenza tra copia clone e copia immagine

La copia clone consiste nella clonazione bit per bit di un supporto di memorizzazione informatico all'interno di un altro dispositivo di memorizzazione della stessa tipologia vergine (il risultato finale sarà un secondo dispositivo di memorizzazione della stessa natura del primo il cui bitstream è precisamente identico al primo).
La copia immagine consiste nella copia bit per bit di un supporto di memorizzazione dove la successione di bit non viene memorizzata in maniera integrale sul supporto di destinazione ma in un file immagine all'interno del supporto stesso.

Analizzando un messaggio di posta elettronica, come è possibile risalire al reale autore?

È possibile risalire al reale autore di una email analizzando gli header del messaggio stesso.
Gli header di un messaggio di posta sono le intestazioni del messaggio stesso e contengono le informazioni relative alla "vita" della mail, dal momento in cui viene inviata all'accettazione da parte del server destinatari. Ad ogni passaggio l'header viene aggiornato in "append", quindi sarà sufficiente

partire dall'alto per identificare il primo sistema che ha generato la mail. Una volta identificato il mittente, sarà possibile richiedere ai provider mail l'utenza (IP) collegata all'account di email nel momento in cui è stato inviato il messaggio, e dall'IP, tramite gli Internet Service Provider, sarà possibile identificare l'utenza telefonica alla quale era assegnato quel determinato IP nel momento di invio della mail.

Cos'è il wiping e quando è necessario in cf?

Il wiping è l'unica modalità che consente di cancellare realmente i dati all'interno di un supporto di memorizzazione, e consiste nell'azzeramento metodico di tutti i bit del supporto. È possibile effettuare un wiping tramite software (su Windows esistono diversi tool preposti, e su Linux esiste il comando "wipe"), o tramite hardware (i copiatori hardware permettono di effettuare il wipe di un supporto).
In CF il wipe è necessario quando si intende "ripulire" un supporto destinato ad uso forense dai dati personali di un consulente o dai dati di vecchi casi, oppure per ri-utilizzare un disco precedentemente scritto per clonarvi un supporto da analizzare, in quanto il wiping è l'unica tecnica che consente di far tornare vergine di supporto.

Applicando hash, firma digitale e marca temporale che garanzie si hanno?

Hash, firma digitale, e marca temporale sono metodologie che consentono di comprovare la legittimità del procedimento seguito per effettuare una acquisizione, e quindi concedere maggiore attendibilità ai riscontri stessi.
Nello specifico, l'hash consente di generare una binary fingerprint del supporto di memorizzazione a livello istituzionale. Il digest di lunghezza fissa generato dagli algoritmi di hashing su sequenze di bit di lunghezza arbitraria individua in maniera univoca l'intero bitstream, essendo questo non invertibile (nonostante esistano le collisioni).
L'applicazione della firma digitale sull'hash consente di garantire l'integrità, l'autenticità ed il non ripudio di un'acquisizione, e garantire così una corretta catena di custodia.
La marca temporale consentirà di documentare il momento in cui è avvenuta un'acquisizione, così rendendo possibile restituire un supporto al proprietario, qualora necessario, e comunque mantenere fondatezza per i riscontri trovati sulle copie forensi oggetto di studio.
Grazie all'utilizzo di queste metodologie sarà possibile rispondere con serenità alle repliche da parte di giuristi e avvocati.

Linux Scripting

Il linguaggio di shell scripting permette di automatizzare attività ripetute, cosa fondamentale per l'amministrazione di un sistema e utile per l'elaborazione dei dati in informatica forense.
Tramite l'esecuzione sequenziale di comandi, sarà possibile effettuare attività di analisi automatizzate, e ottenere riscontri secondo pattern preimpostati.
I comandi eseguiti possono essere interni (built-in) o esterni (file eseguibili esterni, es. /bin).
Lo script è una sequenza di comandi registrabile in un file di testo per poi essere eseguita.
Per eseguire uno script sarà necessario creare il file script (estensione .sh), renderlo eseguibile con chmod, digitare il nome via path.
Tramite un sapiente utilizzo di comandi di shell sarà possibile trovare riscontri in maniera molto specifica e approfondita (ad esempio, utilizzando comandi complessi come "find"), ma si corre anche il rischio di creare un grande inquinamento probatorio (il comando "touch" applicato massivamente, ad es.).

Acquisizione pagina web

L'acquisizione di pagine web deve garantire delle caratteristiche di verificabilità e riproducibilità. Occorre quindi produrre delle copie forensi identiche a quelle originali, ridurre la possibilità di disconoscimento della copia prodotta in giudizio, consentire attività di verifica per controparti, consentire la verifica della genuinità e inalterabilità dell'acquisita prova digitale.
Il procedimento giusto per l'acquisizione di pagine web è quindi il seguente:

1. utilizzo di una macchina virtuale con installato un sistema operativo Linux di tipo forense
2. avvio di una procedura di registrazione audio e video delle operazioni eseguite, utili allo scopo di riprodurle in maniera "semplice" e comprensibile anche per un non tecnico
3. avvio di una procedura di intercettazione del traffico di rete generato dalla macchina virtuale durante le attività di navigazione, utile per acquisire non solo i singoli file scaricati dal browser, ma anche le richieste e le risposte complete dai vari webserver contattati e per documentare in maniera inequivocabile gli indirizzi IP coinvolti
4. consultazione di un sito dal quale poter documentare la data di inizio dell'acquisizione (ad esempio, l'homepage di un quotidiano online)
5. consultazione di tutte le pagine da acquisire utilizzando una procedura di consultazione manuale delle pagine di interesse o di strumenti per acquisizione di porzioni di sito in maniera automatica
6. consultazione di un sito dal quale poter documentare la data di fine dell'acquisizione (ad esempio, l'homepage di un quotidiano online)
7. chiusura della procedura di intercettazione del traffico di rete; chiusura della procedura di registrazione audio e video
8. spegnimento della macchina virtuale
9. generazione di un archivio compresso contenente i file della macchina virtuale, il file della registrazione audio-video, il file di traffico di rete, i singoli file delle pagine web
10. calcolo dell'hash dell'archivio compresso prodotto al punto precedente
11. applicazione di marca temporale all'hash calcolato al punto precedente

Acquisizione mobile con cavetto rotto

Esistono diverse metodologie possibili per far fronte ad un connettore rotto. In ordine di invasività si può:

- Effettuare una acquisizione fotografica dei dati di interesse mostrati tramite il dispositivo stesso
- Cercare di riparare il connettore USB, generalmente distaccato dalle schede madri dei telefoni con un'apertura poco invasiva e quindi procedere con dispositivi di acquisizione come UFED
- Utilizzare i connettori JTAG, per effettuare acquisizione a basso livello elettronico (rischio cifratura coi dispositivi più recenti)
- Effettuare un chip-off del telefono ed effettuare una acquisizione fisica tramite lettore eMMC (rischio cifratura con dispositivi più recenti)

Supertimeline

Le "supertimeline" sono delle timeline che estendono quelle fatte tramite i dati del filesystem prendendo in considerazione anche metadati. A differenza della timeline che si concentra unicamente sulle date di creazione, ultima modifica e ultimo accesso dei file, la supertimeline si concentra sul contenuto dei file per ottenere riferimenti temporali (sfruttando gli artefatti del sistema operativo, come il registro e i file di log, sfruttando i metadati presenti nei file e sfruttando gli artefatti di

navigazione internet, come la cronologia), e fornendo così un prospetto molto più completo sulla storia dei file.

Comando Linux per fare il wiping di un disco

```
dd if=/dev/zero of=/dev/sdX bs=1M
```

Sfruttando il comando DD, sarà possibile effettuare il wiping di un disco (nel comando, andrà sostituita la lettera X con quella del disco di cui effettuare il wiping). Per far ciò sfrutta il file /dev/zero, che non è memorizzato su memoria di massa, essendo virtuale, e ha la particolarità che alla lettura ritorna dei caratteri 0 ASCII, permettendo così l'azzeramento totale del dispositivo indicato in "of".

Come funzionano le BTS? Irradiano segnale in tutte le direzioni?

Una Stazione base di ricezione (BTS) consiste nell'insieme dei ricetrasmettitori e da tutti gli apparati di supporto che forniscono la copertura radio di zona geografica (detta "cella"). La BTS è la parte terminale della rete GSM, infatti ad una BTS afferiscono i dispositivi mobili direttamente, mentre un insieme di BTS afferisce ad un Base Station Controller (BSC). Quando un dispositivo mobile è attaccato ad una BTS, esso sfrutta questa per effettuare le comunicazioni che si appoggiano alla rete mobile (chiamate, messaggi, rete internet), e la BTS di contro tiene traccia dei dispositivi ad essa collegata e alcune informazioni di massima sulle comunicazioni avvenute (numeri chiamati, sms inviati, date e durate delle chiamate…), consultabili poi attraverso la lettura dei tabulati.

Le BTS possono irradiare il segnale in tutte le direzioni qualora le antenne montate su di esse siano "omnidirezionali". In questo caso l'antenna sarà collocata al centro della cella. Le BTS possono però anche irradiare il segnale in maniera "direzionale", trasmettendo il segnale in un lobo direzionale ben preciso, permettendo di coprire sempre e comunque una cella effettiva, ma consentendo così di raggruppare più antenne direzionali in un posto unico e coprire più celle adiacenti.
Questa differenza sarà necessaria per conoscere le BTS implicate durante la lettura di un tabulato telefonico, e tracciare delle linee di handover più precise.

Modalità di acquisizione numeri carte di credito da database di email

Disponendo di un database di email sarà necessario effettuare delle ricerche per pattern in modo da ritrovare un numero di carta di credito.
Considerando che un numero da 16 o 13 cifre, presumibilmente raggruppate in gruppi di quattro, in ambiente linux si potrebbe eseguire una ricerca tramite comando "find" specificando come filtro il pattern del numero di carta di credito, e aggiungere in "or" delle keyword (tipo "credito", o "cc") che possono aiutare ad orientarsi nel database. In ambiente windows vi sono dei programmi a supporto della ricerca efficace (ad esempio, FTK).
La replicabilità del riscontro sarà garantita dalla generazione (e successiva verifica) dell'hash sul database delle email, e quindi dall'applicazione degli stessi comandi di ricerca che hanno consentito di ottenere il riscontro.

Data Carving

Il data carving è una procedura di recupero avanzato dei dati (file e frammenti di file) cancellati. Esso permette di sfruttare il fatto che il file system non sovrascrive i settori allocati per un file cancellato, ma semplicemente ne effettua una deallocazione. Da questo comportamento si generano infatti settori non allocati ma contenenti dati, e slack space (parti di settore non completamente sovrascritte da altri file). Scorrendo tutti i bit del supporto, la procedura di carving cercherà identificare degli header noti per file. Al ritrovamento di uno di questi, procederà con la ricerca del footer relativo a quell'header.

Se nello spazio tra il footer e l'header non si presentano altri header di file cancellati, la procedura ingloberà tutta la sequenza in un file secondo il tipo file interpretato dall'header, diversamente decreterà che il file non è stato allocato contiguamente o è stato sovrascritto, e i dati trovati saranno presentati come frammento di dati.

Acquisizione di un dispositivo mobile

Esistono diverse metodologie di acquisizione di un dispositivo mobile che possono generare riscontri giudicabili come esaustivi, ma che tuttavia non generano una vera e propria copia forense (come nella normale disk forensics).

1. Acquisizione logica: acquisizione che prevede lo sfruttamento del sistema operativo del dispositivo mobile per il recupero e l'analisi dei dati importanti (copia tramite USB, utilizzo del bluetooth, utilizzo della rete). Talvolta, anche tramite questa, è possibile recuperare dati cancellati. Non rispetta il principio di completezza, ma i dati copiati, se ne viene opportunamente documentata la procedura di acquisizioni, sono comunque attendibili.
2. Acquisizione fisica: acquisizione del supporto bit per bit (o quasi). Per fare questa acquisizione in genere servono dei copiatori hardware per cellulare (UFED), e necessita di strumenti software per la lettura di questi dati grezzi.
3. Acquisizione ibrida (tramite agent): si tratta di un metodo di acquisizione ibrida che permette di sfruttare un software installato all'interno del dispositivo per ottenere più dati rispetto alla normale acquisizione logica. Permette di ottenere più dati, ma genera anche un inquinamento probatorio, in quanto va ad alterare il reperto (seppur per pochi mega).

Qualora non sia possibile effettuare una acquisizione nemmeno di tipo logico, sarà possibile acquisire tramite fotografie i dati presentati attraverso il dispositivo stesso.
Esistono poi metodi di acquisizione più invasivi, che lavorano a basso (JTAG) e bassissimo livello (chip-off), con annesso però il rischio di incorrere nell'acquisizione di dati cifrati (UFED per l'acquisizione fisica si occupa di lavorare in modo da aggirare la cifratura), nonché il rischio di compromettere il reperto, qualora non si faccia attenzione.

Acquisizione messaggio whatsapp da telefono con connettore rotto apparte acquisizione manuale tramite video/foto

Esistono diversi metodi di acquisizione logica che possono sfruttare la rete o la connessione bluetooth. Un metodo potrebbe essere l'effettuazione di uno screenshot/registrazione dello schermo e l'inoltro tramite bluetooth ad un altro dispositivo.
Nel caso specifico di whatsapp è possibile effettuare un salvataggio dei dati su cloud. Disponendo dei dati di accesso ai cloud sarà possibile utilizzare un secondo dispositivo sul quale installare whatsapp, farsi inviare un SMS di conferma al numero del telefono da acquisire, accedere a whatsapp e ripristinare il backup, così da avere una copia del messaggio sul secondo dispositivo.

Hash definizione, calcolo e comando linux

L'algoritmo di hash elabora una qualunque mole di bit e restituisce in output una stringa di bit di dimensione fissa (digest). In questo modo è possibile individuare in maniera univoca l'intero contenuto del disco rigido, in quanto l'hash non è invertibile, e così fornire una binary fingerprint di una sequenza di bit (riconosciuta a livello istituzionale).

Il calcolo dell'hash in genere viene effettuato automaticamente dai tool forensi di acquisizione commerciale.
Nel caso del comando "dd" di Linux, questo non viene generato automaticamente, e quindi deve essere calcolato tramite il comando "md5sum", strutturato come segue

```
md5sum /dev/sdX > checksum.txt
```

Questo comando calcolerà l'hash md5 per il disco "sdX" e ne scriverà il risultato dentro il file checksum.txt.

Caratteristica dell'invertibilità dell'Hash

L'hash generato per una sequenza di bit non è invertibile (non è possibile risalire alla sequenza di bit che ha originato l'hash). Questo permette di fare in modo che una sequenza di bit possa essere identificata in maniera univoca attraverso il suo hash. Nonostante ciò, esistono infinite collisioni per un hash (esistono infinite sequenze di bit di lunghezza arbitraria che possono generare lo stesso hash), ma nonostante ciò, lo sforzo computazionale per trovare una collisione è ancora troppo difficile per essere praticato (lasciando il discorso delle collisioni solo su un discorso teorico).

Comando per DD

dd consente di effettuare una copia da un dispositivo di input (if) ad un dispositivo di output (of). Es.

```
dd if=/dev/sda of/mnt/destinazione/img.dd
```

DD ha la proprietà che effettua la copia bit per bit dal dispositivo di input a quello di output. Tramite dd sarà possibile generare una copia clone (clonando il dispositivo di input su quello di output) o generare una copia immagine (generare un file che contenga integralmente il bitstream del dispositivo di input).
In una sua particolare applicazione permette anche di eseguire il wipe di un supporto di memorizzazione:

```
dd if=/dev/zero of=/dev/sdX bs=1M
```

utilizzando come input il file virtuale /dev/zero che consente riempire il dispositivo di destinazione con soli zeri.
DD non calcola di default l'hash dell'acquisizione. Ciò si potrà fare in separata sede, sfruttando il comando "md5sum" oppure utilizzando al posto del comando dd il comando `dcfldd` (che calcola automaticamente l'hash), o ancora utilizzando strumenti commerciali per l'acquisizione, che di norma calcolano l'hash.

Handover e caso pratico

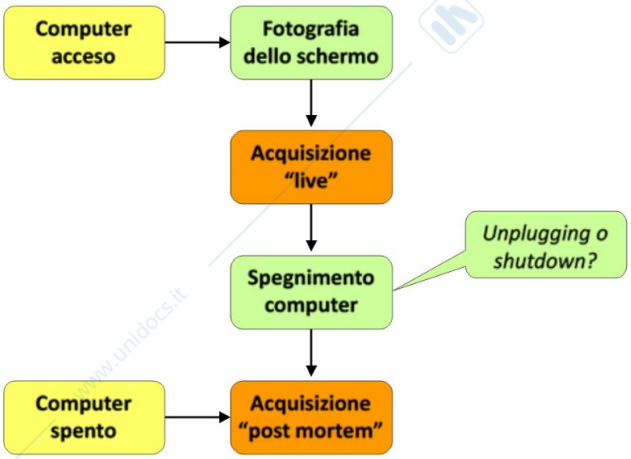
L'handover consiste nella procedura che effettua un dispositivo mobile quando il segnale della BTS a cui è collegato comincia ad indebolirsi (per via della lontananza dall'antenna o per problemi) a favore di un'altra BTS, e quindi si scollega da essa e si collega alla nuova BTS. Questa procedura avviene approssimativamente quando il dispositivo attraversa una linea immaginaria tracciata a equidistanza tra due BTS (detta appunto linea di handover).
L'attraversamento di una linea di handover va tenuta conto quando si effettua la lettura dei tabulati telefonici, in quanto consentirà di avere una geolocalizzazione approssimativa di un dispositivo mobile nel tempo (che dovrà essere però coadiuvata da altri elementi probatori).
Un caso pratico è stato quello dell'alibi informatico. In questo caso vennero posizionate su una mappa le BTS alle quali il cellulare dell'imputato si collegò, e quindi vennero tracciate le linee di handover. Tracciando queste linee fu possibile ricostruire il percorso in macchina che svolse l'imputato, e la successione consecutiva di più eventi sul percorso su più BTS rendeva l'alibi dell'imputato

estremamente attendibile. Tramite successivi accertamenti sulla posizione del veicolo, fu possibile comprovare l'alibi dell'imputato.

Acquisizione Live

L'acquisizione Live prevede invece:

- l'esecuzione di un software apposito
- la connessione del supporto di destinazione al sistema da acquisire
- la copia su supporto di destinazione



Il consulente tecnico dovrà scegliere se fare un unplugging o shutdown, in base al fatto che il shutdown potrebbe comportare un inquinamento del reperto.

Durante l'acquisizione live saranno necessarie alcune verifiche:

- ora di sistema
- cifratura
- registri
- processi in esecuzione
- connessioni attive
- porte aperte