www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

COMPUTER FORENSIC

IMMAGINE FORENSE (copia / bit stream image) diversa dalla copia "logica"

Copia bit a bit da un dispositivo ad un altro; [compresi i dati dello **slack space** (*spazio residuo di un file che è stato* ***sovrascritto*** *parzialmente da un altro; e che nonostante l'eliminazione dell'utente (di tale file) continua a esistere.*]
realizzato mediante copiatori forensi (**Tableau TD3**) o SW per l'acquisizione (**Oxygen** Forensic) con relativo write blocker
Deve essere **STATICA** (immodificabile) controllata dai valori di hash di entrambi i dispositivi.

Realizzata mediante:
CLONAZIONE Non è possibile distinguere l'originale, no compressione/riorganizzazione, si scrive direttamente sul DISCO.
COPIA **IMMAGINE** creazione di un'immagine del disco sorgente in un **FILE all'interno del FS** del disco di destinazione.
E' possibile suddividerla (split) in più file ciascuno [2-4GB] e compressione (**EWF,AFF**) per compattare aree non utilizzate.

mkdir /dest
mount /dev/**sdg2** /dest -o rw
dd if=/dev/**sdd o**f=/dest/immagine.dd If è l'input ; of è l'output copiare l'hard disk sdd nella cartella /dest

➔ Affiancata dalla **CATENA DI CUSTODIA:** è un documento che contiene le informazioni di ciò che è stato fatto con la prova originale e con le copie forensi realizzate da tutti gli "attori" che hanno partecipato, a partire dall'acquisizione fino ad arrivare al giorno del processo. Contente acquisizione completa **dei reperti raccolti**, da chi, descrizione: modello, numero di serie, firma, luogo in cui il supporto è stato rinvenuto, i valori digest (Impronta UNICA con un programma di HASHING con SIGILLO elettronico) , data ora e luogo inizio/fine custodia.
Utile a RICOSTRUIRE il trattamento e **CHI potrebbe aver causato alterazioni.**

CARVING eseguita su una copia forense [i file quando vengono cancellati vengono nascosti in attesa di essere sovrascritti]
Il **data carving** è una tecnica che consente di recuperare file (anche corrotti = danneggiati) da un supporto di memorizzazione di dati digitali (ad esempio un hard disk o una chiavetta USB) anche quando non vi è più traccia di quel file nella tabella di allocazione; ma non i metadati associati quali: dati creazione/modifica/accesso nome/percorso

STEP 1 → **marcato come "eliminato"** ma memorizzato ancora es cestino/camion spazzatura → SW per il ripristino
STEP 2 → Elimino la entry del file nella tabella di allocazione "elimin.definitiva" **FAT** → unico metodo: carving.

FUNZIONAMENTO: SCORRO tutti i bit in maniera sequenziali della copia forense fino a che rilevo un **header** noto: (es pdf %PDF, docx→pk) localizzabile sulla superfice binaria del dispositivo in quanto ha una propria signature), e un **footer** (es EOF) → salvo il contenuto in un pdf;

LIMITI: Non è possibile recuperarlo quando il file è stato **sovrascritto** (non lo recupero in maniera integra), **frammentato in + settori non contigui** sul supporto), non ha un header/footer caratterizzante es: file di testo

BASATA SU cluster, settori e Byte. → **SW: RECUVA for Windows**

QUANDO Non si ha la possibilità di connettersi al dispositivo per MANCANZA DI INTERFACCE, SW non riesce a ACQUISIRE o perché distrutto parzialmente si può applicare la tecnica del:
CHIP-OFF Dissaldatura/estrazione con attrezzature speciali, **dump** (elenco) del contenuto binario e ricostruzione dati / ACQUISIZIONE FOTOGRAFICA /
HW **JTAG** (Join test action group) connettersi alle porte jtag del dispositivo per decodificare e leggere i dati direttamente dal chip.

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

RETE GSM Global System for Mobile Communications

BTS Base **transCEIVER** Station (ricetrasmittente) realizza canali di comunicazioni verso le MS (mobile station: cell)

NSS Network Switching Subsistem → **MSC** mobile switching center //telefonia

BSC controlla BSS e NSS

BSS stazione base coordina onde radio e gestisce frequenze, decide handover

HANDOVER: Spostamento di un MS ad un'altra BTS in caso di (di default)

- **CONFINAMENTO** (Affollamento=densità dispositivi; riduzione consumo energia dispositivo/interferenze, miglioramento qualità; di contro potrebbe connettersi ad una BTS lontana da dove si trova.
- **SALVATAGGIO** (segnale debole, deterioramento segnale es: viaggio ; il vantaggio di proseguire la comunicazione anche in movimento)

→ Esaminando i tabulati può essere interpretato come spostamento geografico sul territorio

Tabulato (lista) telefonico: **IMEI** relativo al cellulare fisico , **IMSI** relativo alla SIM "internazionale"

TIMELINE: Tutte le operazioni eseguite "cronologicamente" sul PC: creazione, ultima modifica/lettura
VERIFICARE GLI HASH TRA I FILES dopo la prima copia e confrontare la timeline per vedere cosa è stato modifcato

CTU Consulente Tecnico UFFICIO → lavora al fianco del giudice scelto da esso o meno (non perforza iscritto all'albo)
CTP di PARTE → presta la propria opera di consulenza alle parti "in causa"(che lo pagano). Figura optional non obbligatoria in quanto protezione "aggiunta" davanti al giudice (coadiuva=aiutare). Accettare consigli assistito.

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari