Computer Forensics

Accertamenti tecnici art 359 cpp: il PM può avere la necessità di svolgere accertamenti tecnici, che comportano specifiche conoscenze scientifiche, tecniche o artistiche, che esulano dalle competenze possedute dall'organo inquirente
Il PM può avvalersi/nominare un Consulente Tecnico

Accertamenti tecnici irripetibili art 360 cpp: Accertamenti che se compiuti comportano l'alterazione della prova e la ripetibilità della procedura non è più garantita; il PM esegue questa attività di accertamento avvisando previamente l'indagato e il suo difensore e la parte offesa e il suo difensore, in modo da dare la possibilità a questi ultimi di assistere a tutta l'operazione a garanzia del rispetto delle procedure, le parti hanno la facoltà di nominare un proprio Consulente Tecnico.

Incidente Probatorio: Viene richiesto per anticipare la formazione di una prova durante le indagini preliminari, il PM e il PG svolgono le indagini con perquisizioni e sequestro probatorio:
V Può essere richiesto dal PM
V Ha lo scopo di formare la prova
V Il GIP può nominare un suo consulente tecnico detto Perito
V Non velocizza il processo, semplicemente anticipa la formazione della prova

Procedimento Penale:
V Si realizza in due strutture: il tribunale e la Procura
V Si instaura con l'iscrizione della notizia di reato
V Si conclude con il giudicato penale
V Si instaura su iniziativa di una parte e anche d'ufficio

Procedimento Civile:
V Le parti in giudizio sono: l'attore ed il convenuto (procedimento ordinario)
V Si realizza in un'unica struttura: Il tribunale
V Le parti in giudizio sono: il ricorrente ed il resistente (procedimento con ricorso)
V Si instaura su iniziativa di una parte: l'attore o ricorrente
V Si instaura esclusivamente su iniziativa di una parte
V Le parti in giudizio possono nominare un consulente tecnico
V Il giudice può nominare un consulente tecnico detto Perito

GIP Giudice per le indagini preliminari:
V Non è l'unico interlocutore del Pubblico Ministero, anche la Polizia Giudiziaria
V Non Emette una sentenza
V Non può emettere sentenza di luogo a non procedere
V Provvede alle misure Cautelari
V Può non accogliere la richiesta di archiviazione

V Non ha autonomia di iniziativa probatoria, solo su richiesta di PM o indagato

GUP Giudice Udienza Preliminare:
V Interviene dopo l'esercizio dell'azione penale
V il GUP può emettere decreto di rinvio a giudizio dopo richiesta del PM di rinvio a giudizio
V il GUP può emettere sentenza di luogo a non procedere alla richiesta del PM di rinvio a giudizio

Il Pubblico Ministero conferisce l'incarico ai sensi dell'art 360 cpp:
V Quando sussiste il rischio che l'elemento probatorio da analizzare possa venire alterato o distrutto in fase di analisi/accertamento
V Indica al Consulente Tecnico che deve eseguire un accertamento NON ripetibile
V Quando il PM intende disporre il dissequestro del materiale sequestrato
V In caso di accertamenti non deve richiedere autorizzazione
V È l'organo con funziona requirente/inquirente

Chi può prendere parte agli accertamenti tecnici ripetibili ai sensi dell'art 359 cpp:
V Il consulente tecnico del PM (CTU), in quanto vige il segreto investigativo

Chi può prendere parte agli accertamenti tecnici non ripetibili ai sensi dell'art 360 cpp:
V Il difensore dell'indagato
V Il difensore dell'indagato accompagnato dal proprio consulente tecnico (CTP)
V il consulente tecnico di parte della persona offesa (CTP)
NOTA BENE: Si parla di indagato non imputato.

Quando si giunge al Giudicato Penale?
V Quando viene emessa la sentenza della Corte di Cassazione
V Quando sono decorsi i termini per proporre opposizione/impugnazione

Quali sono le caratteristiche proprie della Persona Offesa?
V Può nominare un difensore
V Può presentare memorie
V Può sporgere denuncia e fare esposti
V Può interloquire sia nella fase delle indagini preliminari che in quella di giudizio
V Può sporgere querela
V In determinati casi può ritirare la querela
V Può farsi assistere da un consulente tecnico

Esposto: segnalazione di un fatto allo scopo di far valutare se ricorre un'ipotesi di

reato
Denuncia: si dà notizia di reato perseguibile d'ufficio (può essere presentata da chiunque)
Querela: dichiarazione della persona offesa (Non perseguibile d'ufficio)(Può essere presentata solo da coloro che subiscono l'azione penalmente perseguibile)

L'intervento di un Computer Forenser può essere richiesto da:
V Il giudice dibattimentale in composizione monocratica
V Il Pubblico Ministero
V L'indagato
V La Polizia Giudiziaria
V La Parte offesa

La scelta degli strumenti tecnici e delle metodologie che il Computer Forenser deve impiegare nella corretta conduzione della propria opera è dettata da:
V La comunità scientifica

L'indagato/Imputato
La qualità di indagato si conserva fino alla richiesta di rinvio a giudizio o archiviazione
L'imputato è la persona indagata nei confronti della quale è stata esercitata l'azione penale

Entrambi hanno l'obbligo di farsi assistere da un difensore
Avvocato difensore: è nominato da entrambe le parti delle indagini preliminari/processo

V Ha l'obbligo di farsi assistere da un difensore
V Può farsi assistere da un consulente tecnico quando viene eseguito un accertamento tecnico
V Può produrre memorie difensive solo nella fase delle indagini preliminari
V Non ha l'obbligo di farsi assistere da un consulente tecnico quando viene eseguito un accertamento tecnico
V L'indagato assume il ruolo di imputato quando viene esercitata l'azione penale
V Non ha l'obbligo di presentarsi in udienza

Qual è l'ambito di applicazione della Computer Forensics?
V Qualsiasi reato dove possa esistere un sistema informatico coinvolto a questo titolo

La copia forense:
V È una qualunque copia di dati che rispetta le caratteristiche di preservazione e

validazione
V È una qualunque copia di dati eseguita in modo tale da garantire la ripetibilità delle successive operazioni di analisi
V È una duplicazione dei dati eseguita in modo tale da garantire sempre la ripetibilità delle successive operazioni di analisi
V Non è una duplicazione dei dati di interesse investigativo
V Non è una copia bit a bit dell'intero supporto
V Non deve essere eseguita con un write blocker
V Non deve essere sempre eseguita con tool forensi

Il Sequestro fisico:
Consiste nel prendere fisicamente il supporto
V Se il dispositivo è acceso bisogna preoccuparsi del problema dello shut down
V Non è sempre possibile eseguirlo

Il Sequestro Logico:
Consiste nell'eseguire una copia totale o parziale della memoria del dispositivo
V è sempre possibile eseguirlo
V Viene eseguito elaborando la c.d. copia forense
Quindi è una duplicazione dei dati di possibile interesse investigativo, garantisce la ripetibilità dei successivi accertamenti sulla copia stessa
V Se il dispositivo è acceso NON bisogna preoccuparsi del problema dello shut down perché per eseguire la copia il sistema deve essere già avviato

Nella fase di identificazione, la preview:
è un'analisi di primo livello delle memorie dei dispositivi per identificare elementi di interesse investigativo
V è una perquisizione informatica
V NON deve necessariamente essere eseguita realizzando la copia forense, posso anche semplicemente sfogliare il contenuto del reperto.
V Può essere eseguita su un sistema acceso
V è particolarmente utile ad individuare le fonti di prova
V è una fase in cui in alcuni casi vi è il rischio di alterare il reperto, soprattutto in caso di preview LIVE
V NON deve essere sempre eseguita su un sistema aperto
V Possono essere accesi dispositivi rinvenuti spenti, bisogna però considerare le informazioni che saranno perse

La Preview in un sistema acceso (LIVE):
Analisi del sistema attivo, più rapida, più rischiosa, può essere eseguita attraverso programmi di utility in lite mode, Tool ad hoc

V Rende veloce l'analisi dei software presenti nel sistema
V NON può essere eseguita con qualsiasi tool forensics oriented indipendentemente dal sistema da analizzare, bisogna usare tool compatibili con il S.O. del reperto
V NON può essere eseguita con una distro live forensics oriented (solo in caso di DEAD)
V NON è consigliabile usarla con un write blocker (da usare in caso di DEAD)

La Preview in un sistema spento (DEAD):
Analizza il S.O. morto, NON altera la prova attraverso l'uso di write blocker, Un alternativa al write blocker è la distro live forensics oriented
V Deve essere eseguita con un write blocker
V è meno rischiosa di un sistema acceso LIVE
V Se il sistema da analizzare è acceso bisogna analizzare se conviene spegnerlo
V Non può essere sempre eseguita (sistemi embedded come smartphone e router)
V Non velocizza l'analisi dei software presenti nel sistema (Quella è la LIVE)

Per Validazione si intende che:
V I dati della copia forense sono identici ai dati originali
V l'hash della copia forense coincide con l'hash calcolato dal supporto originale
V Non sempre l'hash della copia forense coinciderà con l'hash calcolato da una successiva copia forense (come succede in caso di riavvio con uno smartphone)

Per Preservazione si intende che:
V L'hash della copia forense coincide con l'hash calcolato dalla medesima copia dopo la fase di analisi
V L'hash ricalcolato sulla copia forense varierebbe alla minima alterazione della copia stessa

La c.d. Preview:
V Dovrebbe essere eseguita da tecnici specializzati poiché vi è il rischio di alterazione della prova
V è una fase in cui in alcuni casi vi è il rischio di alterare il reperto
V Può essere eseguita su di un sistema acceso
V Rende veloce l'analisi dei software del sistema
V è uno strumento di ricerca della prova permesso agli inquirenti in sede di perquisizione
V è particolarmente utile ad individuare le fonti di prova
V Il suo uso non è esplicitamente indicato nel Codice penale
V NON deve sempre essere eseguita realizzando la copia forense
V NON permette di eseguire un'analisi completa
V POSSONO essere accesi i dispositivi rinvenuti spenti

V NON è sempre necessario l'ausilio di un write blocker

In analisi, montare un file immagine:
V Implica che il sistema debba riconoscere il FileSystem presente
V è utile per analisi mirate
V è utile per impiegare strumenti non forensics oriented
V Permette l'esportazione del calcolo dell'hash dei file d'interesse
V Permette la visualizzazione immediata dei soli file residenti
V NON Permette la visualizzazione immediata dei file cancellati
V NON Permette di orrente una analisi completa

È un formato per disk image:
V DD
V ISO
V .bin/.cue
V Smart (.s01, .s02, …)

ENCASE L (logical) 01 Bitstream EWF
Acquisizione di tipo logica
15 sezioni
Si ottiene da un file E01 di tipo Disk Image

ENCASE E01 bitstream EWF
Formato basato su Smart
V Permette di conservare i metadati del reperto sorgente
V Permette la compressione (3 livelli: no, good, best)
V è un formato della famiglia Expert Witness Disk Image Format
V Può conservare il calcolo dell'hash
V Non può contenere la copia logia di una cartella/directory

ADVANCED FORENSICS FORMAT (AFF/AFF4)
Formato open, memorizzazione di disk image e relativi metadata associati
Disco separato in due layer:
-Disk-rappresentation layer (metadato)
-Data-storage layer (dato)

Il formato DD/RAW
V Non conserva nei metadati il calcolo dell'hash
V Non conserva alcun metadato del reperto sorgente
V Non permette la compressione
V Rappresenta la copia di un solo "file/steam"

V NON è un formato della famiglia Expert Witness Disk Image Format
V NON può contenere la copia logica di una cartella/directory

Il comando DD

V Esegue una copia bit a bit di un supporto di memoria generando un file immagine
V Permette di eseguire una copia di un solo file/steam
V Da solo non permette di produrre una copia forense (necessità di un write blocker)

Copia Forense: Comandi
dd
if: input file
of: output file
bs: block size in byte (default 512)
conv:
-“no error” continua ad elaborare nel caso di errore di lettura
-“sync” sostituisce i blocchi di memoria non letti nella destinazione con NULLs
skip = [n] salta la lettura del numero n di blocchi di memoria partendo dall’inizio
count = [n] indica all’elaboratore di terminare dopo aver letto il numero n di blocchi di memoria

I toolkit (GUYMAGER e FTK IMAGER)

V Permettono di eseguire la classificazione bad extension confrontando l’estensione del file con la signature in esso presente
V Facilitano il computer forenser nell’individuazione delle informazioni di interesse
V Permettono una ricerca tramite hash
V Eseguono una classificazione dei file
V Processano/elaborano il contenuto del disk image
V Permettono di eseguire il file carving (recupero da spazio non allocato) ricercando l’header ed il footer dei file conosciuti
V Permettono diverse tipologie di visualizzazioni

GuyMager

Tool opensource, si basa sulla libreria “libwf” ovvero AFF
Permette di fare solo una copia full disk elaborando una clonazione o disk image
Formato dell’immagine sarà DD/RAW o EWF(E01)
V Permette di produrre disk image nel formato E01
V è uno strumento per elaborare le copie forensi
V Fa uso dell’hashing on the fly
V Permette di segmentare/splittare il file immagine (è possibile selezionare la dimensione di split)
V Permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256

V Esegue copie forensi solo di tipo “full disk”

FTK Imager

V è uno strumento per elaborare copie forensi
V Riconosce solo determinati tipi di FileSystem
V Permette di visionare il contenuto dei Disk Image
V Non permette la scelta del tipo di Hash da calcolare (Li calcola sempre e sono MD5 e SHA-1)
V Può eseguire una copia della memoria volatile
V Fa uso dell’hashing on the fly
V Permette di segmentare/splittare il file immagine
V Permette di esportare i file di interesse
V Permette di produrre disk image nel formato E01/RAW(DD)/SMART/AFF (Permette la scelta)
V Permette di avere informazioni su alcuni dei file cancellati
(File orphan, file cancellati che non hanno più la cartella che li conteneva)
V Può essere impiegato anche come strumento per la c.d. Preview

Algoritmo di Hash MD5

V Processa il messaggio in blocchi di 512 bit (ogni blocco è fatto da 16 parole di 32 bit)
V È costituito da 4 round e 4 funzioni logiche (MD4 è costituito da 3 round e 3 funzioni logiche)
V Fa uso di 64 costanti additive
V L’output è un digest a 128 bit
V Rispetto a MD4 fa uso di 62 costanti in più

SHS/SHA

Nell’algoritmo di SHA-1 se il messaggio di input M è di 968 bit, dopo il padding avremo che M’ sarà costituito da
V 3 blocchi da 512bit
V un bit “1” al 969 bit
V 1536bit
Nell’algoritmo MD5 se il messaggio di input M è di 1024, dopo il padding M’ sarà costituito da:
V Un bit “1” al 1025bit
V 448 bit di padding

Autopsy

V Permette l’aggiunta di ulteriori moduli di analisi

V Permette una configurazione “multiple user” (server) (single user SQlite)
V Permette la selezione dei file di interesse solo tramite “tag”
V Il “Central Repository” permette di rapportare il caso in esame con i precedenti casi già elaborati
V Il Disk Image viene processato tramite “Ingest Modules”
V Il modulo “Hash lookup” permette di impostare sia una lista di “ignorable file” e sia di “notable file”
V Il File Carving viene svolto tramite il tool “PhotoRec”
V Il modulo “PhotoRec” viene eseguito sullo spazio non allocato
V Il modulo che si preoccupa di estrarre informazioni dal cestino di sistema è “Recent Activity”
V Il modulo “Keyword Search” impiega “Apache Solr”
V Il modulo “Interesting Files” permette di evidenziare i file corrispondenti a determinate regole
V Il modulo “File Extension Mismatch” dipende dal modulo “File Type”
V Il modulo “Encryption Detection” permette di evidenziare possibili file protetti
V Il modulo Virtual Machine Extractor ricerca i file VMDK e VHD e li inserisce in “datasources”
V La sezione “Tags” contiene le annotazioni dell’utente
V Le informazioni dal registro di sistema vengono estratte tramite il tool “RegRipper”
V Il modulo “Exif Parse” estrae i metadati, exif dai file JPEG, memorizzandoli nella sezione Result
V Il modulo “Email Parser” ricerca ed analizza archivi di posta elettronica
V Il modulo “Plaso” elabora una timeline dell’evidence più specifica
V Il modulo “Data Source Integrity” Calcola e valida l’hash del reperto assicurano l’integrità del’’evidence
V Il modulo “Correlation Engine” è una ricerca più approfondita dei file del caso all’interno del “central repository” aggiornandola con i file del caso corrente
V Il modulo “Android Analyzer” analizza i dispositivi android ed estrae registro chiamate, contatti, messaggistica, browser, geolocation etc…

Partizione DOS (DOS PARTITION MBR)

V Contiene sempre un MBR
V Contiene un EBR se ha Secondary Extended Partition
V Può contenere al massimo 4 partizioni primarie
V Il settore contenente l’MBR termina con una signature
V Non ha limite al numero di partizioni che può contenere
V Rispetto al partizionamento GPT può contenere un numero di partizioni inferiore
V La Partition Table nell’EBR è costituita da 4 entry, di cui 2 sono vuote

V La Partition Table è costituita da quattro entry da 16 byte
V MBR è costituito da un settore da 512 byte
V Non contiene sempre una partizione EBR
V Non contiene sempre una MBR e un EBR
V l'EBR NON deve necessariamente contenere al massimo 1 entry

File System

I file system sono un sistema che permette la memorizzazione dei dati, organizzandoli gerarchicamente in file e directory in modo tale da ritrovarli in maniera rapida
-File system category
-Content category
-Metadata category
-File Name category
-Application category

Dati essenziali sono detti Trusted data e che se modificati/alterati causano un malfunzionamento del sistema:
indirizzamento del contenuto del file
nome del file
dimensione del file
Dati Non essenziali sono detti Untrusted Data e sono quindi informazioni accessorie:
dati temporali
permessi utente

Nel File System

V Le informazioni temporali sono dati non essenziali
V I dati non essenziali possono non essere coerenti
V Il FileSystem Category comprende le informazioni sul layout
V In Content Category i dati sono organizzati in data unit
V Il Metadata Category comprende le informazioni sull'indirizzo
V In Application Category sono presenti i dati NON essenziali per alcune funzionalità del FileSystem
V l'indirizzio della data unit dove è memorizzato un file è un dato essenziale
V lo Slack Space indica un settore non utilizzato di data unit allocata
V Il Physical Address (eseguito mediante Logical Block Address) è l'indirizzio del settore calcolato in base al primo settore del volume
V Logical Disk Volume Address è l'indirizzo del settore calcolato in base al primo settore del volume
V Logical Volume Address è l'indirizzo del settore calcolato in base al primo settore della partizione

V La strategia di allocazione del primo disponibile ricerca una data unit libera partendo dall'inizio del FileSystem
V la strategia di allocazione del prossimo disponibile ricerca una data unit libera partendo dall'ultima data unit allocata
V la strategia di allocazione del più adatto ricerca data unit consecutive libere per non frammentare il file da allocare

Nel FAT File system
V Il layout è costituito da:
-Reserved Area che include informazioni sul file system category
-FAT Area che contiene la primary structure del FAT e anche dei backup delle strutture, la sua dimensione è calcolata in base al numero e alla grandezza delle strutture FAT presenti
-Data Area che contiene i cluster da allocare per memorizzare i file e directory
V Le data unit si chiamano cluster
V Nel fat32 la root directory ha dimensione dinamica (valido solo per la FAT32)
V La dimensione delle entry del FAT dipendono dalla tipologia di FAT (Quindi hanno dimensione fissa in base al numero FAT12 = 12 bit)
V Le prime due entry del FAT non sono utilizzate per i cluster, la prima entry della tabella FAT inizia con indirizzo zero, Entry[0] = informazioni del media, Entry[1] = dirty status
V I cluster iniziano con indirizzo due
V lo stato di allocazione dei cluster è conservato nella struttura FAT
V La seconda entry del FAT indica se il FileSystem NON è stato smontato correttamente, oppure eventuali errori Hardware
V Lo stato di non allocazione dei cluster è indicato con ZERO all'interno della FAT
V Lo stato di non allocazione dei cluster è indicato con ZERO e quello di allocazione con l'indirizzo del prossimo cluster o con il marcatore End-Of-File
V La tipologia del FAT non è contenuta in nessun settore, bisogna calcolare i dati presenti nel boot sector
V il FSINFO è una strutta di dati NON essenziali per il FAT32

NEL NTFS
V Una entry MTFS può avere anche più di un attributo di tipo $DATA
V la signature BAAD serve per segnalare un ipotetico errore o corruzione dell'entry
V Lo stato di allocazione dell'entry è definito dall'attributo $BITMAP
V $Standard_information attribute esiste per ogni file e directory e contiene i metadati principali, nulla di questo attributo è essenziale
V $File_Name attribute contiene il riferimento al parent directory che lo contiene, e

permette in analisi di individuare tutto il percorso di una entry casuale
V $DATA attribute viene utilizzato per memorizzare qualsiasi forma di dati, se supera i 700 byte l'attributo diventa non residente
V Il contenuto di un attributo NON residente viene memorizzato in un cluster-run
V In ogni entry MFT di base vi è un attributo $Standard_Information
V In ogni entry MFT di base vi è un attributo di tipo $Attribute_List
V Ogni Entry MFT di base ha anche un attributo di tipo $File_Name
V Le entry MFT vengono pulite non appena il flag in uso viene settato
V La dimensione del cluster è indicata nel Boot Sector del $Boot File
V Nel File $BitMap è indicato lo stato di allocazione di ciascun cluster
V I Cluster danneggiati vengono indicati dal file $BadClus
V Ogni cosa è gestita come file
V Il file $BasClus ha un attributo $DATA della stessa dimensione del FileSystem
V Le informazioni temporali sul file sono contenuto solo all'interno dell'attributo $Standard_Information

Sistemi Operativi

Windows:
HKEY_CLASS_ROOT contiene due tipi di informazioni (dati che permettono di associare, dati di configurazione delle componenti)
HKEY_USERS contiene le impostazioni di tutti i profili utenti configuranti nel sistema (NTuser.dat), ogni sottoalbero di quest'albero descrive ciascun utente
HKEY_CURRENT_USER contiene il puntatore al profilo utente specifico presente in HKEY_USERS loggato nel sistema
HKEY_LOCAL_MACHINE contiene informazioni relative alla configurazione del pc come hardware, sistema operativo, bus, driver
HKEY_CURRENT_CONFIG contiene il puntatore alla corrente configurazione situata in HKEY_LOCAL_MACHINE

ShellBag

Preferenze utente nelle visualizzazione del contenuto delle cartelle
BagMRU: storico di tutte le cartelle visualizzate dall'utente
Bags: contiene solo le impostazioni di visualizzazione delle cartelle contenute in BagMRU(settate dall'utente)

File Swap

Pagefile.sys è un'estensione della memoria RAM
Pagefile.sys del SO Windows si trova nella root del disco
Hiberfil.sys è una copia della RAM quando viene mandato in ibernazione il sistema ed è un vero e proprio dump della RAM

V In SO Windows HKEY_USERS è una hive del registro di sistema che contiene le informazioni dell'utente
V Lo SwapFile o pagefile.sys in un SO Apple è posizionato nel percorso /private/var/vm
V Lo SwapFile in un SO Windows si trova nella root di Windows
V In un SO Windows la gran parte delle impostazioni del sistema e dell'utente sono memorizzate nel registro di sistema
V Il SO Windows è molto meno rigido nella gestione della struttura del FileSystem rispetto ad un SO Linux
V Linux registra molti più log di Windows
Il pagefile.sys rappresenta un'estensione della memoria RAM
V In SO Apple il FileValut offre la funzionalità di cifratura
V L'analisi dei thumbnail viene eseguita per avere informazioni sulle immagini non più presenti
V In Linux i file dell'utente si trovano esclusivamente nella propria home directory
V In un SO Windows i file dell'utente NON si trovano esclusivamente nella propria home directory
V In un SO Windows il file SAM contiene sempre l'elenco di tutti gli account utente che si sono loggati almeno una volta sul sistema
V In SO Windows i thumbnail del sistema NON sono sempre coerenti con i file residenti, potrebbero esserci thumbnail di file non più residenti

Nella Mobile Forensics:
Logical Extraction:
V Nella Logical Extraction NON bisogna preoccuparsi di decodificare i dati estratti
V Nella Logical Extraction i dati sono messi in strutture dati che dipendono dallo strumento di acquisizione
V La Logical Extraction dipende dall'API del dispositivo

Manual Extraction:
V La Manual Extraction si esegue fotografando il contenuto del dispositivo
V La Manual Extraction può essere eseguita su quasi la totalità dei dispositivi
V La Manual Extraction NON è il metodo più veloce per estrarre i dati
V La Manual Extraction NON può essere impiegata in caso di schermo rotto o codice di sblocco

FileSystem Extraction:
V Nella FileSystem Extraction si ottengono i DB così come sono presenti nel dispositivo
V Nella FileSystem Extraction si ottengono i contenuti presenti nel dispositivo a

seconda dei permessi
V Nella FileSystem Extraction bisogna decodificare l’output per visualizzare i dati