

UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

CORSO DI LAUREA IN INFORMATICA

APPUNTI DEL CORSO 2019/2020 DI



COMPUTER FORENSICS

DEGLI STUDENTI CIRO COZZOLINO
ABRAMO CAROTENUTO

Lezione 1

Appunti sulla Computer Forensics

Che cos'è la Computer Forensics?

La Computer Forensics è l'insieme di metodologie scientificamente provate finalizzate alla ricostruzione di eventi ai fini probatori che coinvolgono direttamente o indirettamente un supporto digitale.

Che cos'è la Digital Forensics?

La Digital Forensics è un ramo della scienza forense che comprende il recupero e l'indagine del materiale trovato nei dispositivi digitali, spesso in relazione a eventi di criminalità informatica.

La Computer Forensics è la branca della Digital Forensics che si occupa del trattamento di dati digitali di tipo computer, PC, notebook, hard disk etc da utilizzare come prova in un processo.

Le fasi del trattamento del dato digitale sono :

- ◆ Identificazione (individuare i dispositivi che possono contenere *dati rilevanti*)
- ◆ Raccolta
- ◆ Validazione
- ◆ Preservazione
- ◆ Analisi
- ◆ Interpretazione
- ◆ Documentazione
- ◆ Presentazione

Lezione 2

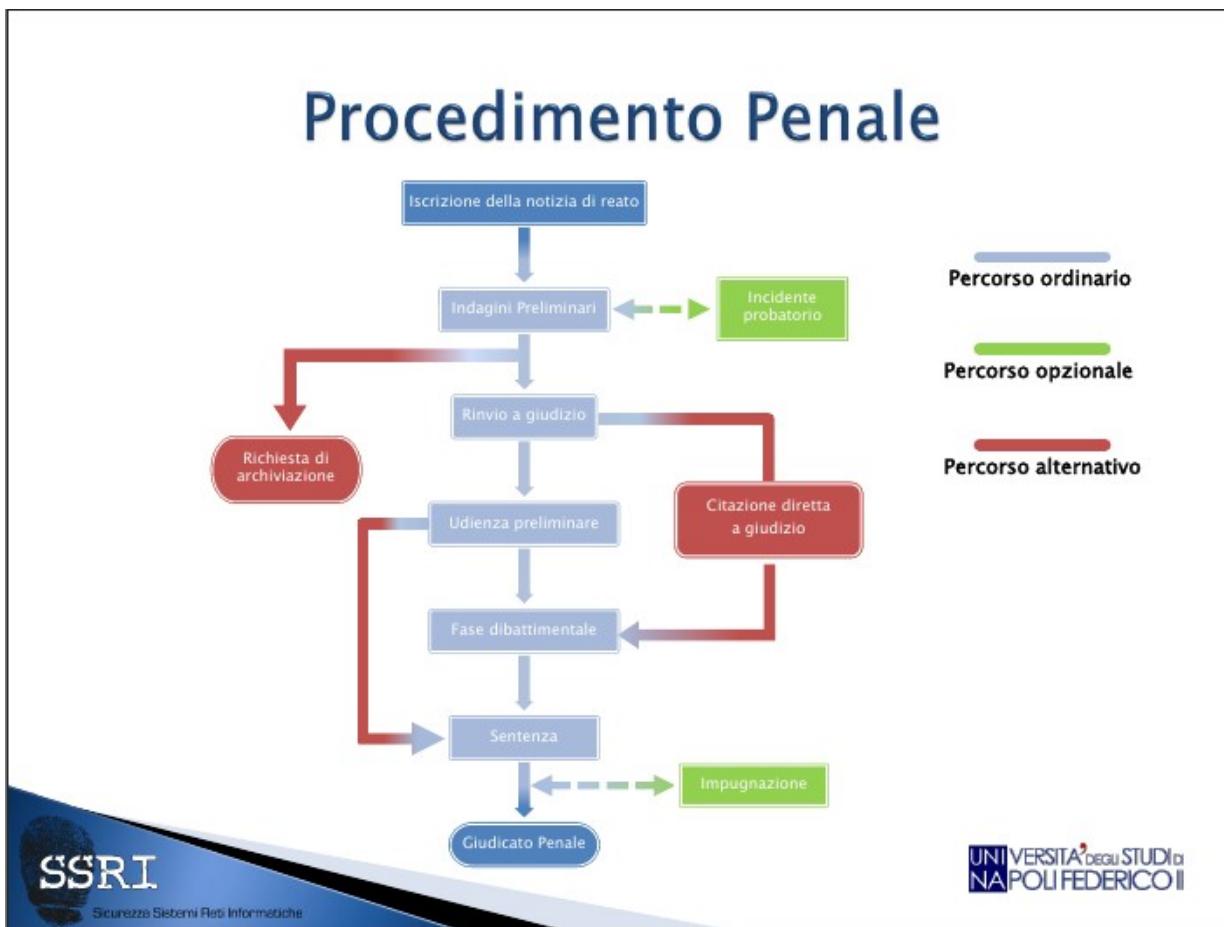
Il procedimento penale e civile

Chi è il Pubblico Ministero(P.M.)? (associato alla Procura della Repubblica)

Il Pubblico Ministero gestisce le indagini ed ha il potere di esercitare l'azione penale.

Chi è il Giudice? (associato al tribunale)

Il giudice valuta le tesi accusatorie e difensive,dunque può condannare o assolvere.



Fasi del procedimento penale.

- *Iscrizione della notizia di reato.*
Un soggetto(persona offesa o testimone) o un'autorità può “denunciare” un reato , e tale notizia di reato è iscritta dal P.M. su un apposito registro dei reati.
- *Indagini preliminari.*
Il P.M. e la polizia giudiziaria(P.G.) svolgeranno le indagini per appurare che il reato sussista.
Durante questa fase il P.M e la P.G. possono far uso di due strumenti giuridici: perquisizione e sequestro probatorio.
La **perquisizione** è utilizzata per verificare la presenza di una prova di reato.

Il sequestro probatorio è utilizzato solitamente in seguito del riscontro positivo della perquisizione ed ha lo scopo di tutelare la prova da possibili alterazioni.

Il P.M. durante questa fase può avere la necessità di svolgere accertamenti tecnici(art 359 cpp) **nominando un Consulente tecnico**(come il digital forensen).

Possono essere svolti anche **accertamenti tecnici irripetibili**(art 360 cpp) che se compiuti comportano l'alterazione della prova e la ripetibilità della procedura non è più garantibile.

E' il P.M. a svolgere questa attività avvisando PRIMA:

- l'indagato e il suo difensore;
- la parte offesa e il suo difensore;

Le parti hanno la facoltà di nominare un proprio *Consulente tecnico*.

- **Incidente probatorio (PERCORSO OPZIONALE)**

Può essere richiesto da entrambe le parti ed ha il compito di anticipare l'acquisizione e la formazione di una prova durante le indagini preliminari.

La richiesta dell'incidente probatorio viene fatta al GIP (*Giudice delle indagini preliminari*).

Nel caso in cui sono previste competenze tecniche il GIP può nominare un proprio consulente tecnico : *il perito*.

- **Richiesta di archiviazione (PERCORSO ALTERNATIVO)**

Al termine delle indagini preliminari il P.M. può presentare una richiesta di archiviazione al GIP nel caso in cui il reato non sussiste e dunque ritiene che non ci siano gli estremi per un rinvio a giudizio.

La parte offesa può presentare una richiesta motivata di *opposizione* al GIP.

- **Rinvio a giudizio**

La richiesta di rinvio a giudizio è l'atto con cui il P.M. esercita l'azione penale.

- **Citazione diretta a giudizio (PERCORSO ALTERNATIVO)**

E' esercitata dal Pubblico Ministero quando si tratta in particolare di delitti puniti con la pena della reclusione non superiore nel massimo a quattro anni.

- **Udienza preliminare**

E' il passaggio dalla fase procedimentale alla fase processuale.

L'indagato si trasforma in *imputato*.

Il GIP viene sostituito dal GUP (*Giudice dell'udienza preliminare*).

L'imputato può richiedere al giudice di essere prosciolto o di rinunciare alla fase dibattimentale (rito alternativo).

- **Fase dibattimentale**

Il dibattimento è la fase centrale del processo penale,nella quale si procede alla raccolta e alle acquisizioni delle prove.

- **Sentenza**

Proscioglimento : sentenza di non doversi procedere o sentenza di assoluzione.

Condanna : è pronunciata quando l'imputato risulta colpevole del reato che gli è stato contestato.

- *Impugnazione* (PERCORSO ALTERNATIVO)

E' lo strumento attraverso il quale una delle due parti nelle quale sia stato emesso un provvedimento giudiziario svantaggioso ne rimette il controllo ad un giudice diverso.

Secondo grado di giudizio (corte d'appello).

Terzo grado di giudizio (corte di cassazione).
- *Judicato penale*
 La decisione sull'imputato non è più modificabile.

Penale VS Civile

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. Diritto Penale; 2. Si realizza in due strutture diverse: Procura e Tribunale; 3. Ha lo scopo di accertare la verità nell'interesse dello Stato e della collettività;

 4. Si instaura anche d'ufficio.

 5. il giudice non si pone una situazione di indifferenza, ma persegue uno scopo ben preciso: accettare la verità del reato; | <ol style="list-style-type: none"> 1. Diritto Privato; 2. Si realizza in un'unica struttura: il Tribunale; 3. Ha lo scopo di verificare l'esistenza di un diritto reclamato da un privato cittadino nei confronti di un altro e quale, tra le due parti in causa, ha ragione; 4. Si instaura esclusivamente su iniziativa di una parte: l'attore 5. il giudice si attiene solo alle prove presentate dalle parti, ponendosi in una posizione di equidistanza e imparzialità (principio dispositivo); |
|---|--|



Lezione 3

Gli attori del procedimento penale

Chi è il Pubblico Ministero(P.M.)?

E' il titolare delle indagini ed ha il compito di esercitare l'azione penale.
Egli rappresenta la pubblica accusa.

Quali sono i poteri del P.M.?

- Il P.M. dirige le indagini preliminari.
- Può avere l'aiuto della Polizia Giudiziaria (P.G.) per trovare prove di accusa verso coloro che commettono reati.
- **Nomina consulenti tecnici.**
- Valuta l'esito delle indagini e decide se archiviare o rinviare a giudizio.
- Esercita l'azione penale, formulando il capo di imputazione e sostiene in giudizio la tesi accusatoria.

Cos'è la Polizia Giudiziaria(P.G.)?

Sono forze di polizia che collaborano con il P.M. nelle attività di indagini preliminari.

Che ruoli ha la P.G.?

- *Attività informativa* : acquisisce la notizia di reato e la riporta al P.M.
- *Attività investigativa* : ricerca dell'autore del reato
- *Attività di prevenzione* : impedisce che i reati vengano aggravati
- *Attività assicurativa* : individua e protegge le fonti di prova

Chi è la persona offesa?

E' il soggetto titolare del bene giuridico leso dall'autore di un reato.

Può presentare memorie ed indicare elementi di prova, e **nominare** un difensore e **consulenti tecnici**.

Terminologie.

- **Esposto** : è la segnalazione all'autorità giudiziaria di un fatto allo scopo di far valutare se ricorre un'ipotesi di reato.
- **Denuncia** : è un atto con il quale si informa l'autorità giudiziaria di un reato perseguitabile d'ufficio.
- **Querela** : è una dichiarazione della persona offesa con la quale si esprime la volontà di punire il colpevole per un reato subito, non perseguitabile d'ufficio.

Chi è l'indagato?

L'indagato è la persona nei cui confronti vengono svolte le indagini a seguito dell'iscrizione di un fatto a lui addebitato nel registro delle notizie di reato. La qualità d'indagato si conserva fino alla richiesta di archiviazione o di rinvio a giudizio.

Ha l'obbligo di farsi assistere da un difensore.

Può avvalersi di consulenti tecnici.

Chi è l'imputato?

L'imputato è la persona indagata nei confronti del quale è stata esercitata l'azione penale (rinvio a giudizio).

Ha l'obbligo di farsi assistere da un difensore.

Non è obbligatoria la sua presenza in udienza.

Può avvalersi di consulenti tecnici.

Che ruolo ha l'avvocato(difensore)?

Egli ha un ruolo di assistenza e rappresentanza.

E' nominato sia dalla parte offesa sia dalla parte indagata/imputata.

Può ottenere un accesso agli atti delle indagini preliminari.

Che funzione ha il Giudice dell'indagine preliminare(G.I.P.)?

Ha la funzione di *garanzia dell'indagato* nella fase delle indagini preliminari.

Può decidere se accogliere le richieste del Pubblico Ministero.

Ha la funzione di *garanzia dell'azione penale*, ossia può accogliere o meno la richiesta di archiviazione.

E' privo di un proprio fascicolo.

Che funzione ha il Giudice dell'udienza preliminare(G.U.P.)?

Egli interviene dopo l'esercizio dell'azione penale.

Giudica la richiesta di rinvio a giudizio, emettendo decreto di rinvio a giudizio oppure emettendo sentenza di non luogo a procedere.

Il C.F. nel Procedimento Penale: *le indagini preliminari*

- se sono richieste particolari competenze tecniche, può essere nominato dall'autorità giudiziaria un *consulente tecnico* (art. 348 c. 4 c.p.p)

Pubblico Ministero



Consulente
Tecnico d'Ufficio
(CTU)

Polizia Giudiziaria



Ausiliario
di P.G.

Computer Forensen

Qual'è il ruolo del Computer Forenser?

Il C.F. deve impiegare metodi e strumenti che garantiscono **l'inalterabilità della prova**, anche se non dettagliatamente descritti dalla legge.

Per quanto riguarda gli accertamenti irripetibili (accertamenti che se compiuti possono portare all'alterazione della fonte di prova) nel caso del CF va effettuato ad esempio per dispositivo non in buono stato o per esigenze di restituzione del reperto (dispositivi fondamentali per la normale attività di un'azienda).

Il C.F. nel Procedimento Penale:

accertamento irripetibile (art. 360 cpp)

- il P.M. esegue questa attività di accertamento avvisando preventivamente l'indagato 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. L'indagato può nominare e farsi assistere un proprio Consulente Tecnico: Consulente Tecnico di Parte (CTP).



Il C.F. nel Procedimento Penale:

Perito

- In caso di un incidente probatorio o di un'udienza, in cui sono richieste particolari competenze tecniche, il Giudice può nominare un Consulente Tecnico: il Perito.
- può essere scelto dall'Albo del Tribunale oppure da soggetti non iscritti, se individua in questi particolare competenza tecnica; il perito viene avvistato degli obblighi e responsabilità che assume con il giuramento.



Il C.F. nel Procedimento Penale: riepilogando...

- Il **Computer Forenser** a seconda da chi e da quando viene incaricato assume ruoli diversi all'interno del procedimento:
 - Ausiliario di P.G.:** quando il consulente tecnico è incaricato dalla Polizia Giudiziaria durante determinate operazioni;
 - Consulente Tecnico d'Ufficio (CTU):** quando il consulente tecnico è incaricato dal Pubblico Ministero (PM) durante le indagini preliminari per svolgere determinati accertamenti;
 - Consulente Tecnico di Parte (CTP):** quando una delle parti coinvolte nel procedimento (indagato/imputato e/o persona offesa) incaricano un proprio consulente tecnico:
 - per assistere a presentare prove tecniche del reato subito (*parte offesa*)
 - per controbattere a determinate operazioni tecniche compiute dalla parte accusatoria (*indagato*)
 - Perito del Giudice:** quando il Giudice ha bisogno di compiere determinati accertamenti tecnici o valutare quelle compiute dalle parti;

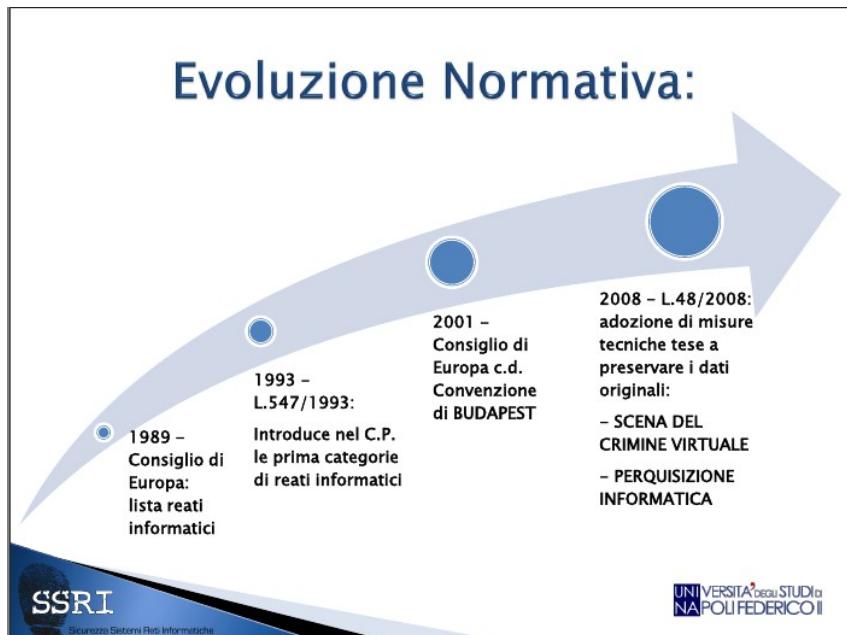
Lezione 4

Genesi del diritto informatico

Definizione di Reato informatico:

A livello internazionale si è rinunciato a dare una definizione vera e propria di reato informatico.

Si è preferito concordare una tipologia di comportamenti ai quali dare l'etichetta di reati informatici.



Nel 1989 vengono elaborate due liste di abusi:

- ◆ **Lista minima** : condotte criminose che gli Stati devono reprimere mediante una sanzione penale.
 - **Frode informatica**
 - *falso in documenti informatici*
 - *danneggiamento di dati e programmi*
 - **Accesso non autorizzato ad un sistema informatico.**
- ◆ **Lista facoltativa** : comportamenti non eccessivamente offensivi, la cui repressione è rimandata alla valutazione dei singoli Stati.
 - **alterazione di dati o di programmi (senza danneggiamento)**
 - **spionaggio informatico.**

Legge n. 547 del 23/12/1993

art. 615-ter c.p.

(Accesso abusivo a un sistema informatico o telematico)

- › Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
- › La pena è della reclusione da uno a cinque anni:
 - 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
 - 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
 - 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.



Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI
NAPOLI FEDERICO II

Legge n. 547 del 23/12/1993

art. 615-ter c.p.

(Accesso abusivo a un sistema informatico o telematico)

- › Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
- › Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio



Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI
NAPOLI FEDERICO II

Legge n. 547 del 23/12/1993

art. 640-ter c.p.

(*Frode informatica*)

- Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire 100 mila a 2 milioni (*cinquantuno euro a milletrentadue euro*).
- La pena è della reclusione da uno a cinque anni e della multa da lire 600 mila a 3 milioni (*euro 600 a euro 3.000*) se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
- Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante

SSRI

Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI
NAPOLI FEDERICO II

Nel 2001 a Budapest ci fu il Consiglio di Europa con il primo trattato internazionale sulla criminalità informatica.

Tra le infrazioni che vennero delineate c'erano :

- le violazioni dei diritti d'autore
- la frode informatica
- la pornografia infantile
- le violazioni della sicurezza della rete

Legge n. 48 del 18/03/2008

- L'Italia recepisce le direttive del Consiglio d'Europa del 2001:
 - **danneggiamento informatico** (c.p. artt. 635-bis, 635-ter, 635-quater, 635-quinquies):
 - distinzione tra danneggiamento dell'integrità dei dati e il danneggiamento dell'integrità del sistema;
 - differenziazione a seconda che l'oggetto della tutela abbia, o meno, rilevanza a fini pubblicistici.
 - **ridefinizione di documento informatico** (art. 491-bis c.p.);
 - **gestione della scena del crimine informatica** (c.p.p. artt. 244, 247, 248, 254-bis, 256, 259, 260, 352, 353, 354)

SSRI

Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI
NAPOLI FEDERICO II

Lezione 6

Fasi del trattamento : identificazione e raccolta

Che cos'è l'identificazione?

L'identificazione è la prima fase del trattamento del dato digitale.

Durante questa fase vengono individuati tutti i dispositivi(computer,cellulari,hard disk,server) che possono contenere dati rilevanti.

Che cos'è la preview(perquisizione informatica)?

La preview è una fase dell'identificazione che consente di eseguire un'analisi di primo livello delle memorie dei dispositivi allo scopo di individuare possibili elementi di interesse investigativo.

Con la preview c'è il rischio di alterazione dei dati con conseguente dispersione di una possibile prova.

Preview “dead” :

E' un'analisi che viene eseguita con il Sistema Operativo spento(non è detto che anche il dispositivo analizzato sia spento) e consente di utilizzare diversi strumenti per analizzare la memoria del dispositivo.

E' previsto l'uso del **write block** che permette di non alterare il dispositivo da analizzare.Per questo motivo è prevista una buona conoscenza del sistema e dei software da analizzare.

Il software che è utilizzato come write block può essere una distro live Linux(CAINE). La “dead” non è praticabile per i sistemi **“embedded”**.

Preview “live” :

E' un'analisi che viene eseguita impiegando il Sistema Operativo presente sul dispositivo da analizzare e consente di avere una visione dell'ambiente in cui opera l'utente.

E' veloce nell'analisi dei software installati e deve essere documentata e verbalizzata.

I contro della “live” possono essere l'alterazione del reperto e l'utilizzo dei strumenti adeguati al sistema.



Cambiamento di stato del dispositivo :

- ◆ **Shutdown** (da acceso a spento)

Prima di eseguirlo bisogna valutare le seguenti criticità :

- Cifratura
- Software in esecuzione
- Dump della RAM

Come si può spegnere il dispositivo?

- Scollegarlo dalla rete elettrica (potrebbe compromettere il funzionamento del sistema)

- Eseguire lo spegnimento mediante il S.O. (vengono eseguite diverse operazioni sul disco come gli aggiornamenti)

- ◆ **Accensione** (da spento ad acceso)

Valutare se le informazioni che perderemo sono meno importanti dell'urgenza dell'accertamento.

Che cos'è la raccolta?

La raccolta è la seconda fase del trattamento del dato digitale.

In seguito all'identificazione dei dispositivi o di dati di possibile interesse investigativo si procede con il **sequestro** che può essere:

- ◆ **Logico**

viene eseguita una copia parziale o totale della memoria del dispositivo.

- ◆ **Fisico**

viene preso fisicamente il dispositivo su cui il dato di possibile interesse risiede, posticipando le problematiche relative all'acquisizione del dato.

Importante in questo la cosiddetta "catena di custodia".

Il sistema fisico **non è sempre fattibile**, in quanto ci sono sistemi che non possono essere fermati/spentti.

La Raccolta: *la catena di custodia*

- ▶ Uno o più documenti (verbale/i) in cui devono essere riportati tutte le informazioni sul dispositivo che è stato sottoposto a sequestrato (fisico o logico):
 - Luogo, data e operatore che ha reperito e collezionato la fonte di prova;
 - Luogo, data e operatore che ha gestito e/o esaminato la fonte di prova;
 - Chi ha la responsabilità della custodia delle digital evidences.
 - Metodo di conservazione del reperto;
 - Eventuali trasferimenti di location dell'evidenza

Che cos'è la copia forense?

La copia forense è una duplicazione di dati di possibile interesse investigativo con la proprietà di validazione e preservazione.

Che cos'è l'acquisizione fisica?

L'acquisizione fisica è una copia bit a bit dell'intero supporto di memoria.

Può essere :

- ◆ **Clonazione**

Ha come risultato un supporto pressoché identico a quello originale.

E' facilmente alterabile e bisogna analizzarne il supporto solo reinserendolo nel proprio habitat.

- ◆ **File immagine**

Ha come risultato un file rappresentante il supporto originale.

E' maneggevole.

Lezione 7

Fasi del trattamento : validazione e preservazione

Cosa fa un algoritmo HASH?

L'algoritmo restituisce una stringa a lunghezza fissa di esadecimali a partire da un flusso di bit(dati) di dimensione qualsiasi.

La stringa prodotta in output è univoca per ogni file e ne è un identificatore.

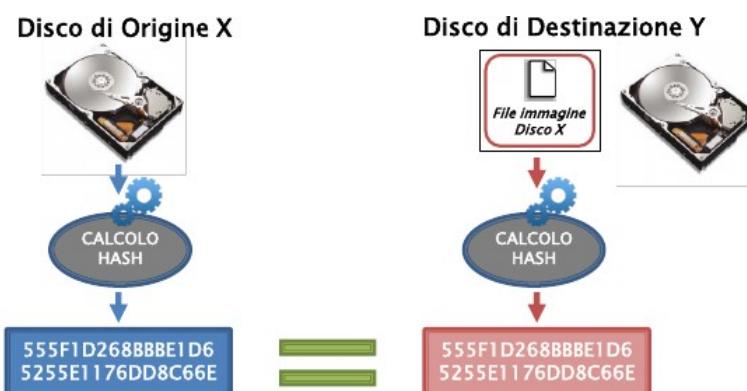
L'algoritmo non si può invertire.

Una *collisione hash* è una situazione che avviene quando due diversi input producono lo stesso output tramite una funzione hash.

Una funzione che prende in ingresso input di lunghezza arbitraria e ritorna un hash di misura fissa(come MD5) deve avere necessariamente delle collisioni,perche il numero di output è finito a fronte di un numero infinito di possibili input.

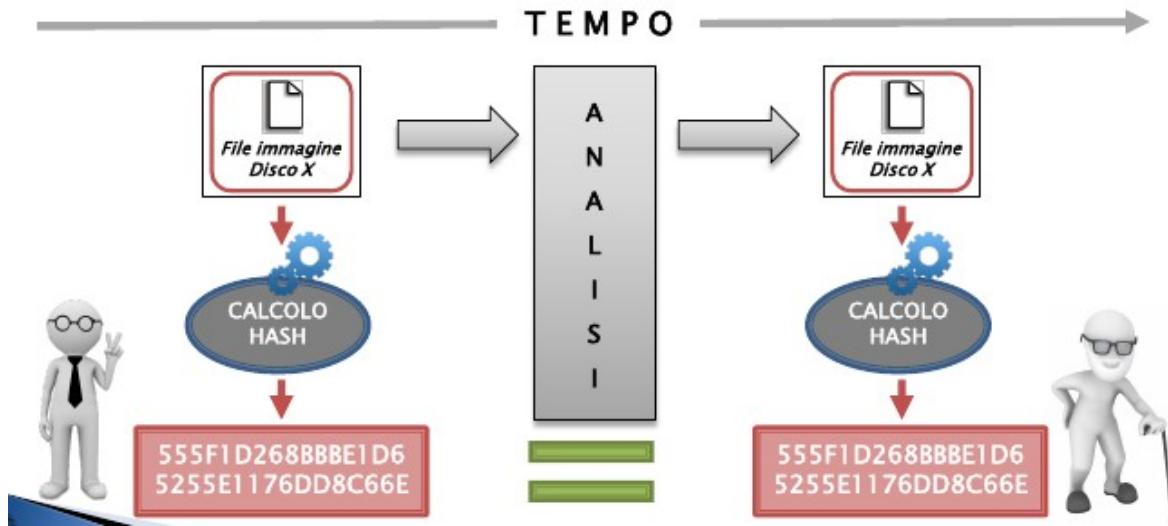
Definizione di validazione :

La validazione garantisce che la copia eseguita è identica al dato originale.



Definizione di preservazione :

La preservazione garantisce che non vengano eseguite modifiche oppure alterazioni alla copia forense. Se ciò avviene l'hash cambierà.



Che cos'è il file LOG?

E' un file descrittivo in cui sono presenti le informazioni sulla copia forense realizzata.

Informazioni del tipo : strumento impiegato(nome,versione) , informazioni del disco origine, altre informazioni(Hash).

Comando DD :

Copia Forense comando «DD»

- ▶ È presente nella gran parte di tutte le distribuzioni UNIX Like

```
DD(1)                                         User Commands
NAME      dd - convert and copy a file
SYNOPSIS  dd [OPERAND] ...
          dd OPTION
```

/dev

tutti i file al suo interno rappresentano dispositivi:

- **Character device:** dispositivi che trasmettono/trasferiscono dati
 - *dsp[0]: dispositivo audio*
 - *lp[0]: porta parallela*
- **Block device:** dispositivi che memorizzano/conservano dati
 - *hd[a]: hard disk ide*
 - *sd[a]: hard disk scsi, memory stick, memory card, etc.*

► Lista dei dispositivi agganciati:

```
root@caine:/# fdisk -l
```

```
Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: dos  
Disk identifier: 0x72a3c36c
```

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sda1		2048	2099199	2097152	1G	b	W95 FAT32
/dev/sda2		2099200	8388607	6289408	3G	b	W95 FAT32

Disco target

```
Disk /dev/sdb: 20 GiB, 21474836480 bytes, 41943040 sectors  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Preparazione copia forense :

- Prepariamo il nostro disco di destinazione della copia forense:

```
root@caine:/# mkdir /mnt/dest  
root@caine:/# mount /dev/sdc1 /mnt/dest/  
root@caine:/# mkdir /mnt/dest/dd_image
```

Comando d'esecuzione per la copia forense :

- Eseguiamo la copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
```

IF = input file [*disco sorgente «sda»*]

OF = output file [*file immagine «sda.dd»*]

BS = block size in byte (default 512) [*dimensione del blocco di lettura «2048 byte»*]

CONV = esegue l'elaborazione in base ai parametri indicati

noerror = continua ad elaborare in caso di errore di lettura

sync = sostituisce i blocchi di memoria non letti nella destinazione con NULs (mantiene sincronizzata la dimensione della destinazione con quella della sorgente)

► Comandi avanzati:

SKIP = *[n]* salta la lettura del numero «*n*» di blocchi di memoria, partendo dall'inizio

COUNT= *[n]* indica all'elaborazione di terminare dopo aver letto il numero «*n*» di blocchi di memoria

Acquisizione di una partizione specifica :

► Acquisire una sola partizione

```
Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device     Boot   Start   End Sectors Size Id Type
/dev/sda1        2048 2099199 2097152  1G b  W95 FAT32
/dev/sda2      2099200 8388607 6289408  3G b  W95 FAT32

root@caine:/# dd if=/dev/sda2 of=/mnt/dest/dd_image/sda_p2.dd bs=2048
572352+0 records in
1572352+0 records out
3220176896 bytes (3,2 GB, 3,0 GiB) copied, 238,845 s, 13,5 MB/s

root@caine:/# ls -l /mnt/dest/dd_image/
total 3144704
-rwxrwxrwx 1 root root 3220176896 apr  7 23:36 sda_p2.dd
```

► Acquisire una sola partizione

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda_p2.dd skip=2099199 count=6289408
6289408+0 records in
6289408+0 records out
3220176896 bytes (3,2 GB, 3,0 GiB) copied, 764,928 s, 4,2 MB/s

root@caine:/# ls -l /mnt/dest/dd_image/
total 3144704
-rwxrwxrwx 1 root root 3220176896 apr  7 23:55 sda_p2.dd
```

Divisione del file immagine :

► Dividere il file immagine:

Blocchi da 1GB (1024 Byte x 1.000.000)

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.000 bs=1024 count=1000000
10000000+0 records in
10000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 200,268 s, 5,1 MB/s

root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.001 bs=1024 skip=1000000
count=1000000
10000000+0 records in
10000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 226,651 s, 4,5 MB/s

root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.002 bs=1024 skip=2000000
count=1000000
10000000+0 records in
10000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 213,783 s, 4,8 MB/s
```

► Dividere il file immagine:

```
root@caine:/# dd if=/dev/sda bs=2048 | split -d -b 2G - mnt/dest/dd_image/sda.
```

► SPLIT

- **-D** = indica di appendere al nome del file un contatore decimale [*sda.00*]
- **-B** = [*n/n(K/M/G/T/P/E/Z/Y)*] specifica la dimensione massima di ciascuna parte [2GB]

```
2097152+0 records in  
2097152+0 records out  
4294967296 bytes (4,3 GB, 4,0 GiB) copied, 157,836 s, 27,2 MB/s  
root@caine:/# ls -l /mnt/dest/dd_image/  
total 4194304  
-rwxrwxrwx 1 root root 2147483648 apr 8 00:12 sda.00  
-rwxrwxrwx 1 root root 2147483648 apr 8 00:13 sda.01
```

Calcolo Hash :

► Metodo nr. 1:

- Calcoliamo l'hash del dispositivo sorgente «**sda**» e lo memorizziamo in un file «**sda_orig.hash**»

```
root@caine:/# md5sum /dev/sda > /mnt/dest/dd_image/sda_orig.hash  
root@caine:/# cat /mnt/dest/dd_image/sda_orig.hash  
d7a09df1018710f2b40744ba62445c7b /dev/sda
```

- Calcoliamo l'hash dell'immagine «**sda.dd**» ottenuta in precedenza ed anche esso lo memorizziamo all'interno di un file «**sda_dd.hash**»

```
root@caine:/# md5sum /mnt/dest/dd_image/sda.dd > /mnt/dest/dd_image/sda_dd.hash  
root@caine:/# cat /mnt/dest/dd_image/sda_dd.hash  
d7a09df1018710f2b40744ba62445c7b /mnt/dest/dd_image/sda.dd
```

- Oppure se la nostra immagine è divisa in più file, dovremo adoperare **CAT**:

```
root@caine:/# cat /mnt/dest/dd_image/sda.* | md5sum >> /mnt/dest/dd_image/sda_merge.hash  
root@caine:/# cat /mnt/dest/dd_image/sda_merge.hash  
d7a09df1018710f2b40744ba62445c7b -
```

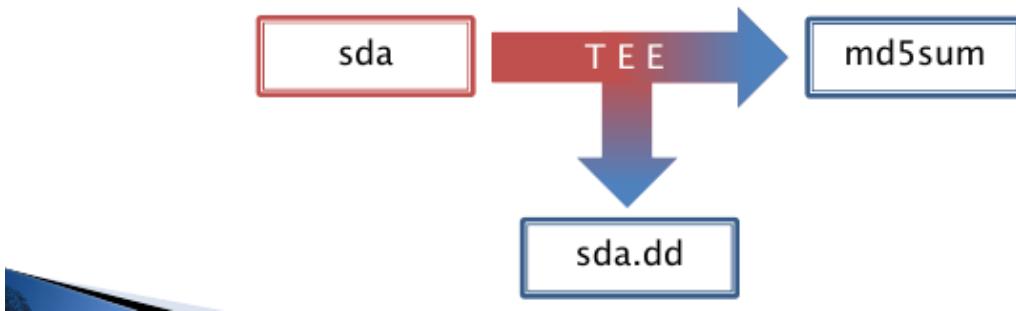
Hash dispositivo di origine = Hash file immagine
(to match)

► Metodo nr. 2:

- Calcoliamo l'hash durante l'elaborazione della copia

```
root@caine:/# dd if=/dev/sda bs=2048 | tee /mnt/dest/dd_image/sda.dd |  
md5sum > /mnt/dest/dd_image/ sda.hash
```

TEE = biforca\duplica lo stream [una viene utilizzata per generare il file immagine, l'altra viene trasmesso al comando successivo «md5sum»]



Comando DC3DD :

► Patch del comando DD

```
root@caine:/# dc3dd if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G bufsz=2k hash=md5  
hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on
```

OFS = output diviso in più file [*file immagine «sda.000»*]

OFSZ = dimensione massima di ogni file [2 GB]

BUFSZ = **BS** = block size in byte (default 512) [*dimensione del blocco di lettura «2048 byte»*]

HASH = [MD5|SHA1|SHA256|SHA512] calcola dell'Hash indicato [**MD5 e SHA256**]

LOG = salva il report dell'elaborazione in un file [**sda.log**]

VERB=ON indica di generare un report dettagliato (verbose)

► Comandi avanzati:

REC=OFF interrompe l'elaborazione in caso di un errore di lettura di un blocco di memoria

HOFS= l'output viene diviso in più file e per ciascuno di essi viene calcolato l'hash;

Lezione 8

Raccolta e Validazione : Disk Image e Tool

Evidence mutevole (art 360 c.p.p.)

Nel caso di un dispositivo che può cambiare stato il calcolo dell'Hash effettuato per la validazione è l'*hashing on the fly* perché così facendo vengono elaborate contemporaneamente sia la copia forense che il calcolo dell'hash in modo tale da avere un match positivo.

Formato DD / RAW :

E' un formato semplice ed è un container dello stream.

Tra le problematiche del formato DD / RAW ci sono :

- non conserva metadati dell'evidence (modello , seriale , dimensione);
- non conserva hash calcolati;
- non esegue compressione;
- non può contenere più di un file / stream(si intendono i dispositivi).

Formato Expert Witness Disk Image Format (EWF) :

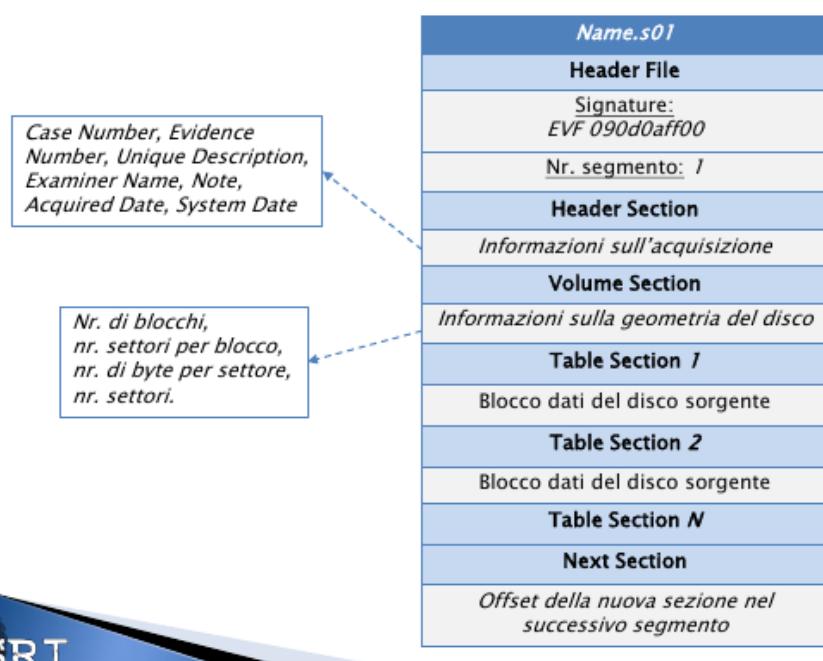
E' un formato di file immagine composto in sezioni :

- esegue compressione;
- segmentazione dell'immagine.

Formato SMART (Famiglia EWF) :

E' un formato che ha l'obiettivo di dare un accesso veloce ad una parte dell'immagine:

- segmentazione dell'immagine;
- ogni segmento è composto da 4 tipi di sezioni.



Formato Encase E01 Bitstream (Famiglia EWF)

E' basato sul formato SMART :

- segmentazione dell'immagine;
- tre livelli di compressione;
- ogni segmento è composto da 13 sezioni.

Formato Encase L01 Logical (Famiglia EWF) :

- acquisizione di file logici;
- segmentazione dell'immagine;
- ogni segmento è composto da 15 sezioni.

Formato Advanced Forensics Format (AFF / AFF4) :

- formato open ed estensibile;
- creato prima dell'implementazione open source di libewf (libreria per il formato EWF).
- ogni disco viene separato in due layer (disk-rappresentation layer , data-storage layer).

Che cos'è Guymager?

Guymager è un tool di acquisizione con licenza open source su piattaforma Linux. Ed è basato sulla libreria "libewf".

Come primo passaggio questo tool ci permette di scegliere attraverso un'interfaccia grafica il dispositivo dalla quale acquisire l'immagine o clonare.

Quali sono le caratteristiche di Guymager?

Le caratteristiche sono : (in grassetto le azioni obbligatorie)

- ◆ **Permette di scegliere il formato dell'immagine (DD/Raw o EWF).**
- ◆ Permette di scegliere la dimensione dei segmenti (split).
- ◆ Scelta dell'HASH (MD5 – SHA1 – SHA256).
- ◆ Calcolo dell'hash del file immagine
- ◆ Calcolo dell'hash del dispositivo sorgente dopo l'acquisizione.
- ◆ Fa uso dell'Hashing on the fly.

Al termine dell'elaborazione Guymager ci fornisce un file .info contenenti tutte le informazioni del file immagine.

Che cos'è FTK Imager?

FTK Imager è un tool di acquisizione su piattaforma Microsoft Windows.

Come primo passaggio questo tool ci permette di scegliere attraverso un'interfaccia grafica il tipo di acquisizione e successivamente il dispositivo da acquisire.

Quali sono i tipi di acquisizione?

- ◆ **Physical Drive**
Copia da un dispositivo fisico.
- ◆ **Logical Drive**
Acquisizione di un supporto ottico.
- ◆ **Image File**
Conversione di un file immagine da un formato ad un altro.
- ◆ **Content of folder**
Acquisizione logica di file in una determinata cartella
- ◆ **Fenico Device**

Quali sono le caratteristiche di FTK Imager?

Le caratteristiche sono : **(in grassetto le azioni obbligatorie).**

- ◆ **Permette di scegliere il formato dell'immagine (DD/Raw , SMART , E01 , AFF).**
- ◆ Permette di scegliere la dimensione dei segmenti (split).
- ◆ Permette di scegliere il livello di compressione del file immagine.
- ◆ Cifratura del file immagine
- ◆ Calcolo e verifica dell'Hash del file immagine con il dispositivo target.
- ◆ Generazione di un file CSV di tutti i file e cartelle presenti.

Al termine dell'elaborazione Guymager ci fornisce un file .txt contenenti tutte le informazioni del file immagine.

E' possibile effettuare il dump della memoria volatile.

Custom Content Image :

Permette di effettuare l'elaborazione di un immagine personalizzata selezionando i file di interesse investigativo.

Si possono utilizzare anche le *wild card* , che sono dei filtri testuali in cui è possibile inserire un percorso di una cartella o un file in formato completo o parziale.

E' possibile filtrare i file da aggiungere all'immagine personalizzata scegliendo i proprietari (*filter by file owner*).

Lezione 9 Protocolli crittografici : Funzioni di hash(parte 1)

Che cos'è un protocollo?

Un protocollo o schema definisce le interazioni tra le **parti**(entità coinvolte nello schema) per ottenere le **proprietà di sicurezza**(segretezza e autenticità) desiderate. Un protocollo si basa su una serie di protocolli più semplici detti **primitive crittografiche**.

- Le primitive risolvono i seguenti problemi :
- cifratura (cifrari simmetrici o asimmetrici);
 - autenticazione ed integrità (funzioni hash e MAC);
 - firme digitali.

Cifrari :

Un cifrario prende in ingresso in chiaro un messaggio di N bit e attraverso una chiave restituisce un messaggio cifrato di N bit.

- ◆ **Simmetrico**

Le parti condividono la stessa chiave. Il messaggio viene letto dal destinatario attraverso la stessa chiave utilizzata dal mittente.

- ◆ **Asimmetrico**

Si impiegano due chiavi :

- chiave pubblica : impiegata per cifrare
- chiave privata : impiegata per decifrare.

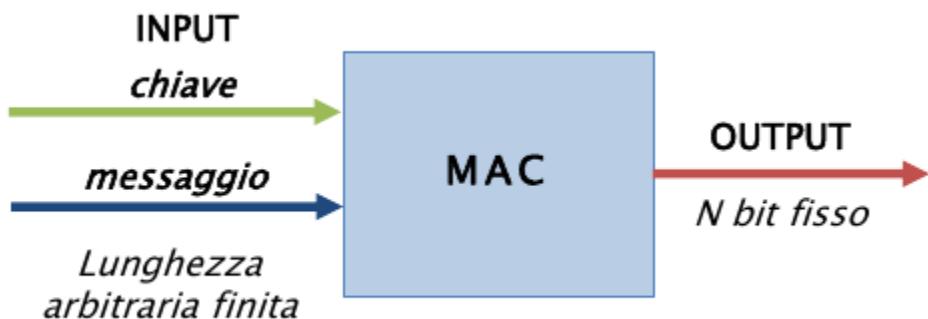
Funzione hash :

Il valore hash $h(M)$ è una rappresentazione non ambigua e non falsificabile del messaggio M.



L'impiego della funzione hash è per garantire **l'integrità dei dati**.

Funzione MAC (Message Authentication Code) :



Impiego :

- integrità dei dati
- autenticità dei dati : verificare chi è stato il mittente dei dati.

Proprietà di sicurezza :

- ◆ **Confidenzialità**
Protezione del dato da un soggetto estraneo.
- ◆ **Autenticazione**
Certezza di identificare l'interlocutore
- ◆ **Integrità**
Verificare che il messaggio non è stato modificato durante la trasmissione.
- ◆ **Non – ripudio**
Negare il disconoscimento del messaggio al mittente o al destinatario.
- ◆ **Anonimia**
Nascondere l'identità di chi ha compiuto una determinata azione nel contesto crittografico.

Collisione :

La funzione Hash è una funzione che ha come dominio un messaggio con lunghezza arbitraria e come codominio un messaggio con lunghezza fissa. Possono esistere **infinite collisioni**.

$$h: \Sigma^* \rightarrow \Sigma^n$$

$$h(m_1) = h(m_2)$$



Esistono infinite collisioni

Proprietà della funzione Hash:

- ◆ **One – way (pre-image resistant) :**
Dato un hash y , è computazionalmente difficile trovare $M \mid y = h(M)$.
- ◆ **Sicurezza debole (2nd pre-image resistant) :**
dato M è computazionalmente difficile trovare una variazione di M , $M' \mid h(M) = h(M')$.
- ◆ **Sicurezza forte (collision resistance) :**
è computazionalmente difficile trovare 2 diversi messaggi con lo stesso valore di hash.

One-Way Hash Function (OWHF) :

E' una funzione che verifica le proprietà di one-way e sicurezza debole.

Collision Resistant Hash Function (CRHF) :

E' una funzione che verifica la proprietà di sicurezza forte.

Funzione One-Way :

Se per ogni x del dominio di f è facile calcolare $y = f(x)$, ma dato y è computazionalmente inammissibile trovare $x | y = f(x)$.

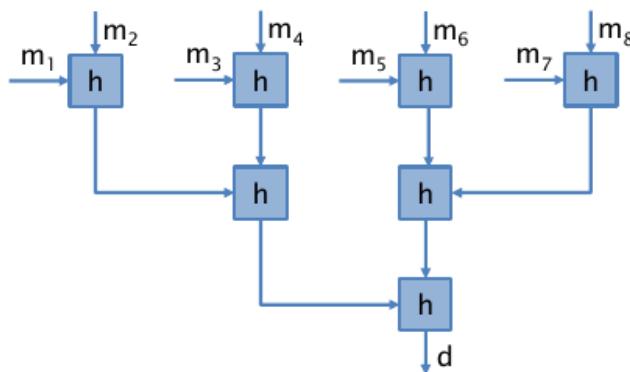
A differenza della OWHS, non ci sono limitazioni sul codominio e non è richiesta la sicurezza debole.

Costruzione della funzione hash :

Il messaggio di lunghezza arbitraria M che prende in ingresso la funzione di hash viene trattato come input fisso, ovvero il messaggio M viene diviso in k blocchi di lunghezza fissa.

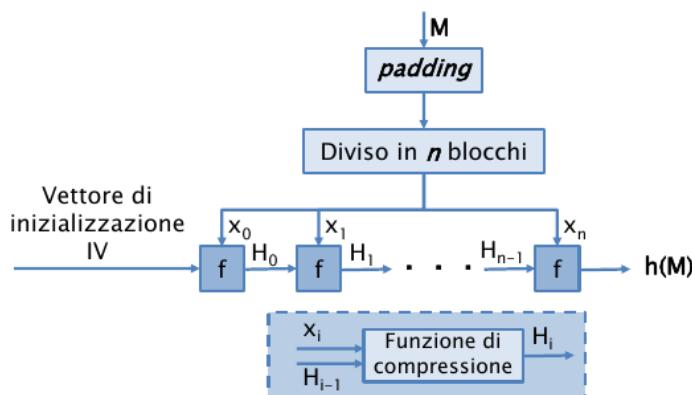
I blocchi vengono trattati in modo **seriale/iterato o parallelo**.

Modello hash parallelo :



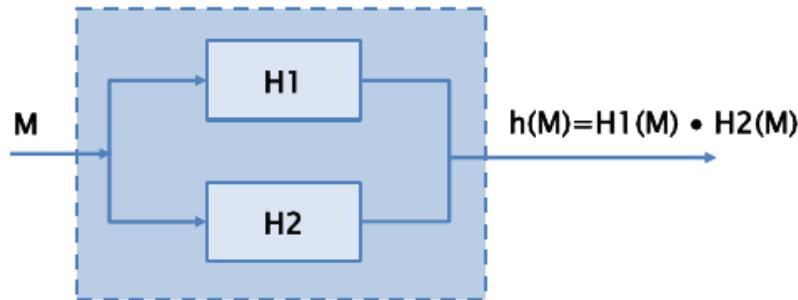
E' resistente alle collisioni se lo è la funzione h .

Modello hash iterato :



Una collisione per $h(M)$ implica una collisione di f .

Modello hash a cascata :



Una collisione per $h(M)$ vuol dire trovare una collisione sia per H_1 che per H_2 .

Lezione 10 Protocolli Crittografici : Funzioni di hash(parte 2)

Funzione Hash MD4 & MD5 :

Le operazioni sono efficienti su architetture 32 bit little-endian.
L'output è 128 bit.

Che cos'è un'architettura little-endian?

E' un'architettura in cui il byte con indirizzo più basso è quello meno significativo.

Che cos'è un'architettura big-endian?

E' un'architettura in cui il byte con indirizzo più basso è quello più significativo.

Quali sono gli obiettivi di MD4 / MD5 ?

- ◆ Sicurezza forte
- ◆ Sicurezza diretta
- ◆ Velocità
- ◆ Semplicità e compattezza

Procedimento :

MD4 / MD5 processa il messaggio in blocchi di 512 bit.

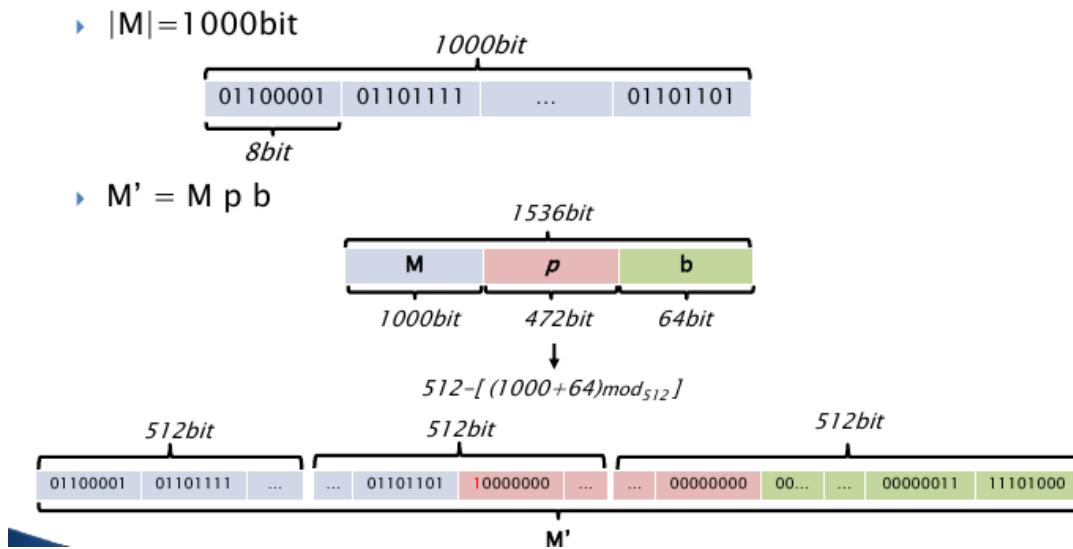
Ogni blocco consta di 16 parole di 32 bit.

M' sarà costituito da :

- messaggio ordinario M ;
- p bit di padding;
- b bit di rappresentazione della lunghezza di M (max 2^{64}).

M' consta di un numero di bit multiplo di 512, ovvero di un numero L blocchi di 512

bit. Ovvero di **N** parole con N multiplo di 16. L = N/16 blocchi di 512 bit. (formula inversa)



Operazioni MD4 / MD5 :

Sia MD4 / MD5 hanno funzioni definite su parole di 32 bit.

- ▶ **MD4/5 impiegano diverse operazioni sulle word in input X e Y restituendo una nuova word:**
 - $(X \wedge Y)$: **and** bit a bit di X e Y
 - $(X \vee Y)$: **or** bit a bit di X e Y
 - $(X \oplus Y)$: **xor** bit a bit di X e Y
 - $(\neg X)$: **complemento** bit a bit di X
 - $(X + Y)$: somma intera modulo 2^{32}
 - $(X << s)$: **shift** circolare a sinistra di s bit

Tutte le operazioni sono molto veloci

Differenze MD4 / MD5 :

- ◆ **MD4**
 - 3 round = $3 * 16$ operazioni (ogni round sono 16 operazioni);
 - 3 funzioni logiche;
 - 2 costanti additive;
- ◆ **MD5**
 - 4 round = $4 * 16$ operazioni (ogni round sono 16 operazioni);
 - 4 funzioni logiche;
 - 64 costanti additive;
 - ogni passo aggiunge il risultato del passo precedente.

Funzione Hash SHA :

Le operazioni sono efficienti su architetture di 32 bit big-endian.
 Stessi principi di MD4 e MD5 ma più sicuro.
 L'output è 160 bit.

Procedimento :

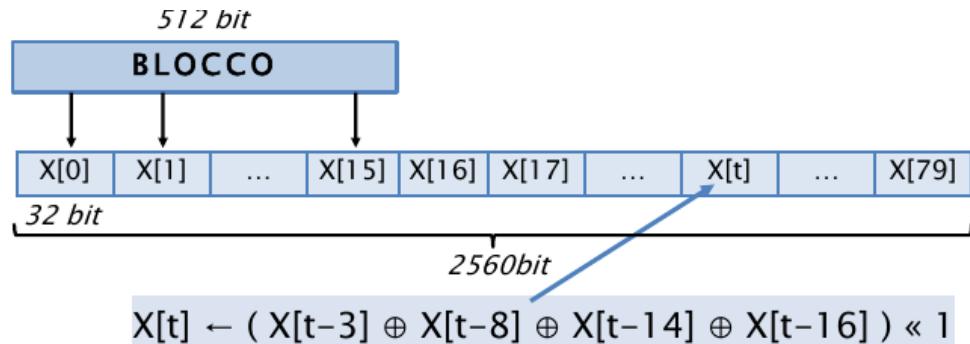
SHA processa il messaggio in blocchi di 512 bit.

Ogni blocco consta di 16 parole di 32 bit.

M' sarà costituito da :

- messaggio ordinario M;
- p bit di padding;
- b bit di rappresentazione della lunghezza di M (max 2^{64}).

M' consta di un numero di bit multiplo di 512, ovvero di un numero **L** blocchi di 512 bit. Ovvero di **N** parole con N multiplo di 16. $L = N/16$ blocchi di 512 bit. (formula inversa).



4 **round** di 20 operazioni ciascuna.

Per ogni iterazione una parola $X[i]$ viene calcolata dal blocco input.

4 **costanti t additive**.

Differenze tra SHA -1 vs MD4 / MD5

- ◆ **Sicurezza forte**
maggiore in SHA-1 (160 contro 128);
- ◆ **Sicurezza contro l'analisi**
MD5 è soggetta ad alcuni attacchi;
- ◆ **Velocità**
entrambi algoritmi molto veloci; SHA-1 ha più passi (80 contro 64) e il buffer ha 160 bit rispetto ai 128 bit di MD5.
- ◆ **Semplicità e Compattezza**

Stessi principi di MD4,MD5,SHA1

SHA 256: Messaggio diviso in blocchi di 512 bit, parole da 32 bit.

SHA 512: Messaggio diviso in blocchi di 1024 bit , parole da 64 bit.

SHA 384: Valore hash = primi 384 bit di SHA-512 con costanti iniziali cambiate.

Lezione 12

L'analisi : gli strumenti (parte 1)

Cosa fa l'analisi?

L'analisi viene eseguita su una copia e può essere riprodotta.

Lo stesso risultato di un'analisi è ottenibile da diverse operazioni / strumenti appropriati.

Permette di ricostruire gli eventi passati mediante la lettura dei dati digitali.

Montare un file immagine

- ◆ Linux (tramite riga di comando)

Analizziamo il file immagine:

► Analizziamo il file immagine

```
root@caine:/# fdisk -l /mnt/dest/dd_image/sda.dd

Disk /mnt/dest/dd_image/sda.dd: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c

Device           Boot   Start     End Sectors Size Id Type
/mnt/dest/dd_image/sda.ddp1      2048 2099199 2097152  1G b  W95 FAT32
/mnt/dest/dd_image/sda.ddp2 2099200 8388607 6289408  3G b  W95 FAT32
```

Il file immagine rappresenta una memoria con due partizioni: p1 e p2

Montiamo la partizione p2

Device	Boot	Start	End	Sectors	Size	Id	Type
/mnt/dest/dd_image/sda.ddp1		2048	2099199	2097152	1G	b	W95 FAT32
/mnt/dest/dd_image/sda.ddp2		2099200	8388607	6289408	3G	b	W95 FAT32

```
root@caine:/# mount -o ro,loop,offset=1074790400 /mnt/dest/dd_image/sda.dd /mnt/sda_dd
```

ro : read-only

loop : crea un virtual book device da un file

offset=byte : punto di inizio della partizione da montare.

Solo immagini DD/RAW non segmentate

affuse : comando per merge(AFFLIBv3).
ewfmount : comando per merge(libewf).

► merge immagine segmentata DD\RAW (AFFLIBv3)

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194308
-rwxrwxrwx 1 root root 2147483648 apr  8 01:16 sda.000
-rwxrwxrwx 1 root root 2147483648 apr  8 01:23 sda.001
-rwxrwxrwx 1 root root      823 apr  8 01:23 sda.log

root@caine:/# affuse /mnt/dest/dd_image/sda.000 /mnt/sda_fuse
root@caine:/# ls -l /mnt/sda_fuse/
total 0
-rw-r--r-- 1 root root 4294967296 gen  1 1970 sda.000.raw

root@caine:/# fdisk -l /mnt/sda_fuse/sda.000.raw
Disk /mnt/sda_fuse/sda.000.raw: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device        Boot   Start     End Sectors Size Id Type
/mnt/sda_fuse/sda.000.raw1            2048 2099199 2097152   1G b W95 FAT32
/mnt/sda_fuse/sda.000.raw2        2099200 8388607 6289408   3G b W95 FAT32
```

► merge immagine segmentata EWF (libewf)

```
root@caine:/# ls -l /mnt/dest/e01_image/
total 235526
-rw-r--r-- 1 root root 104857600 apr  8 02:26 sda.E01
-rw-r--r-- 1 root root 104857600 apr  8 02:28 sda.E02
-rw-r--r-- 1 root root 31457280 apr  8 02:29 sda.E03
-rw-r--r-- 1 root root      7161 apr  8 02:29 sda.info

root@caine:/# ewfmount /mnt/dest/e01_image/sda.E01 /mnt/sda_fuse
root@caine:/# ls -l /mnt/sda_fuse/
total 0
-rw-r--r-- 1 root root 4294967296 apr  8 02:31 ewf1

root@caine:/# fdisk -l /mnt/sda_fuse/ewf1
Disk /mnt/sda_fuse/ewf1: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device        Boot   Start     End Sectors Size Id Type
/mnt/sda_fuse/ewf1p1            2048 2099199 2097152   1G b W95 FAT32
/mnt/sda_fuse/ewf1p2        2099200 8388607 6289408   3G b W95 FAT32
```

◆ **Linux (tramite GUI)**

Il tool utilizzato è IMG_MAP.

◆ **Windows (tramite PassMark OFSMount)**

Attraverso questo tool possiamo montare un file immagine scegliendo la partizione.

◆ **Windows (tramite FTKImager AccessData)**

Attraverso questo tool possiamo montare un file immagine scegliendo la partizione.

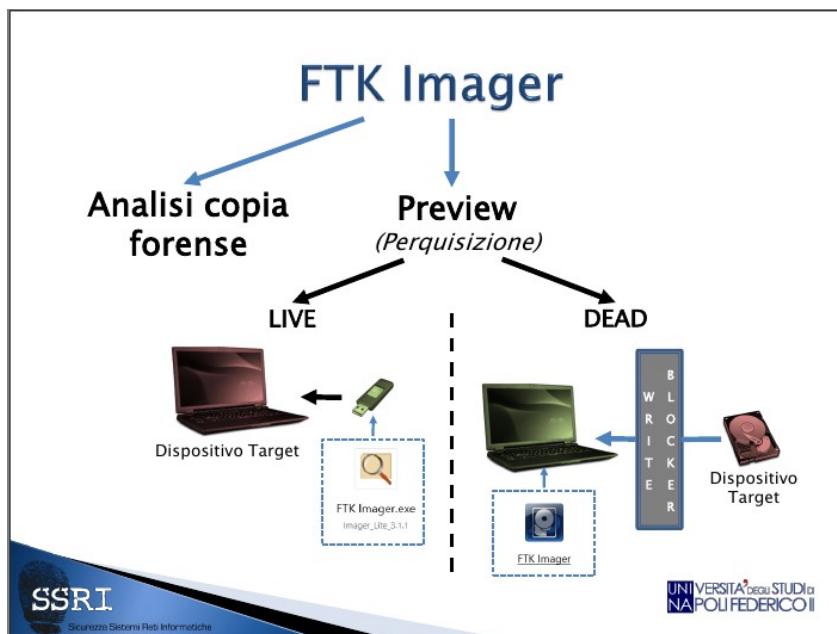
PRO e CONTRO (solo per specifiche analisi) :

- PRO :

veloce per operazioni semplici;
utilizzo di tool non forensic oriented;

- CONTRO :

farraginoso
solo file residenti
riconoscimento del filesystem dell'immagine demandata al nostro S.O.



L'analisi del file immagine mediante FTK Imager :

Attraverso AccessData FTK Imager si può analizzare un file immagine spuntando la voce "Add Evidence Item" scegliendo tra i vari tipi di acquisizioni.

Successivamente FTK Imager ci mostra le informazioni del file immagine attraverso una schermata "header info"(dove è memorizzato anche l'hash dell'immagine alla voce MD5 Verification Hash).

Permette di verificare la proprietà di **preservazione** attraverso " Verify Drive / Image".

Dal punto di vista grafico, la GUI di FTK Imager è divisa in :

- evidence tree;
- file list;
- properties;
- viewer (che è divisa in *internet explorer mode* , *text mode* , *hex mode*).

Tra i **comandi** ci sono:

- Export files (esportazione di un file o un nodo di cartelle)
- Export file Hash List (esportazione del calcolo Hash MD5/SHA1 di un file o di un nodo di cartelle)
- Export Directory Listing (esportazione dell'elenco di file e cartelle presenti nell'interno dispositivo / partizione).

Strumenti software per l'analisi :

◆ **Toolkit**

Supporto dell'intera fase di analisi.

FTK Imager, Autopsy, Passmark OS Forensics.

◆ **Tools Forensic Oriented**

Esecuzione di uno specifico task.

◆ **Tool Generici**

Non progettati per la C.F.

Hard Disk Format :

The following table lists AccessData Imager-identified and analyzed hard disk image formats:

Identified and Analyzed Hard Disk Image Formats

- | | |
|----------------------------------|-----------------------------------|
| • Encase, including 6.12 | • SnapBack |
| • Safeback 2.0 and under | • Expert Witness |
| • Linux DD | • ICS |
| • Ghost (forensic images only) | • SMART |
| • AccessData Logical Image (ADI) | • Advanced Forensics Format (AFF) |

CD – DVD Format :

The following table lists AccessData Imager-identified and analyzed CD and DVD image formats:

Identified and Analyzed CD and DVD File Systems and Formats

- | | |
|----------------------|--------------------|
| • Alcohol (*.mds) | • IsoBuster CUE |
| • PlexTools (*.pxi) | • CloneCD (*.ccd) |
| • Nero (*.nrg) | • Roxio (*.cif) |
| • ISO | • Pinnacle (*.pdi) |
| • Virtual CD (*.vc4) | • CD-RW, |
| • VCD | • CD-ROM |
| • DVD+MRW | • DVCD |
| • DVD-RW | • DVD-VFR |
| • DVD+RW Dual Layer | • DVD-VR |
| • BD-R SRM-POW | • BD-R DL |
| • BD-R SRM | • CloneCD (*.ccd) |
| • HD DVD-R | • HD DVD-RW DL |
| • SVCD | • HD DVD |

File System Format :

The following table lists AccessData Imager-identified and analyzed file systems:

Identified and Analyzed File Systems

- | | |
|-----------------------|-------------|
| • APFS | • HFS |
| • CDFS | • HFS+ |
| • exFAT | • NTFS |
| • Ext2FS | • ReiserFS3 |
| • Ext3FS | • VXFS |
| • Ext4FS | • XFS |
| • FAT12, FAT16, FAT32 | |

Lezione 13

L'analisi : gli strumenti (parte 2)

Formati file immagine dei toolkit :

Forensic ToolKit (FTK)

- ▶ Encase E01
- ▶ Encase L01 Logical Image
- ▶ Expert Witness
- ▶ SnapBack
- ▶ Safeback 2.0 and under
- ▶ ICS
- ▶ Linux DD
- ▶ SMART
- ▶ Ghost (forensic images only)
- ▶ MSVHD (MS Virtual Hard Disk)
- ▶ AccessData Logical Image (AD1)
- ▶ Lx0, Lx01
- ▶ DMG (Mac)
- ▶ VMDK (VmWare Disk)

Autopsy

- ▶ Encase E01
- ▶ Raw (DD, BIN, IMG)
- ▶ Virtual Disk (VMDK, VHD)

Formati file system dei toolkit :

Forensic ToolKit (FTK)

- ▶ FAT
- ▶ exFAT
- ▶ NTFS
- ▶ Ext2FS
- ▶ Ext3FS
- ▶ Ext4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ CDFS
- ▶ ReiserFS 3
- ▶ VxFS (Veritas File System)

Autopsy

- ▶ FAT
- ▶ ExFAT
- ▶ NTFS
- ▶ EXT2FS
- ▶ EXT3FS
- ▶ EXT4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ YAFFS2

Cosa sono le viste?

Le viste sono un elaborazione di file e artefatti e offrono più visualizzazioni delle informazioni contenute nella copia forense.

Tipologie di viste :

- ◆ **Albero**

Rappresentazione gerarchica dei file.

- ◆ **File Type**

Analisi dei file per : estensione(.pdf , . zip) e signature (sequenza di bit posta in un punto ben preciso del file che serve per definire il formato in cui dati sono memorizzati).

I file type vengono analizzati ed arrichiti di nuovi attributi :

- bad extension

- delete file (file marcati come cancellati dal file system)

- ◆ **Known file**

Riconoscimento del file basato sull'HASH(attraverso hash table).

- ignorable file (file conosciuti come di non interesse ,es. quelli di sistema)

- notable file (file conosciuti come di notevole interesse,es. Pedopornografia)

Cosa sono gli artefatti?

Sono un estrazione ed elaborazione delle informazioni presenti in uno o più file.

Artefatti : Metadati

Dati strutturati contenenti informazioni aggiuntive sul file. (" proprietà di un file ")

Per esempio Exif : informazioni sulla fotografia.

Artefatti : e-Mail Archive

Analisi degli archivi/database e-Mail :

- visualizzazione delle mail

- estrazione degli allegati.

Artefatti : System information

Estrazione delle informazioni dell'ambiente di lavoro (sistema operativo).

Artefatti : User Activity

Analisi delle attività eseguite dall'utente (file di registro , log).

Artefatti : Navigazione Web

Analisi dei file dei browser web : history,cookies,cache,download,search.

Autopsy fa l'analisi solo dei seguenti browser web : Chrome,Firefox,Explorer.

Le viste specializzate :

- ◆ **Image gallery**

Generazione e visualizzazione di thumbnail dei file grafici.

- ◆ **Video gallery**

Processo di elaborazione dell'estrazione e visualizzazione di frame dai video.

- ◆ **Social Analyzer**
Visualizzazione delle relazioni/connessioni avvenute tra i diversi soggetti (eMail).
- ◆ **Timeline**
Visualizzazione temporale dei file

File carving :

E' il recupero dei file non più residenti nel file system.

Ricerche semi manuali :

-ricerca tramite attributi;
-document content : estrazione di determinate informazioni mediante regular expression;
- indexing : ricerche di determinate parole chiave;

Altri strumenti :

- Decrypt;
- Malware Analysis;
- Processing Image;
- Traduttore.

Lezione 14

L'analisi : Autopsy (prima parte)

La configurazione di Autopsy :

Autopsy può essere configurato per il singolo utente (*single user*) o per più utenti (*multi user*).

Central Repository :

E' un database in cui vengono memorizzate le informazioni di casi che sono stati precedentemente analizzati.

Ci permette di conoscere file già rinvenuti ed evidenzia automaticamente un file come di notevole interesse(*notable file*).

Central Repository conserva:

- valore (hash,indirizzi mail,numeri di telefono);
- caso;
- data source;
- file path;
- commento del CF;
- notable status.

Rende il case DB più leggero.

Attraverso il menu di gestione delle proprietà di correlazione è possibile configurare la central repository in modo tale da abilitare una o più proprietà di correlazione(file,domains,email address,phone numbers) da usare durante l'analisi.Queste proprietà sono globali e comprendono tutti gli utenti della central repository.

Creazione del caso :

Con Autopsy è possibile creare un nuovo caso aggiungendo le informazioni relative al caso ed è possibile selezionare i moduli da utilizzare.

Formati supportati da Autopsy :

Disk Image:

- ▶ Encase E01
- ▶ Raw (DD, BIN, IMG)
- ▶ Virtual Disk (VMDK, VHD)

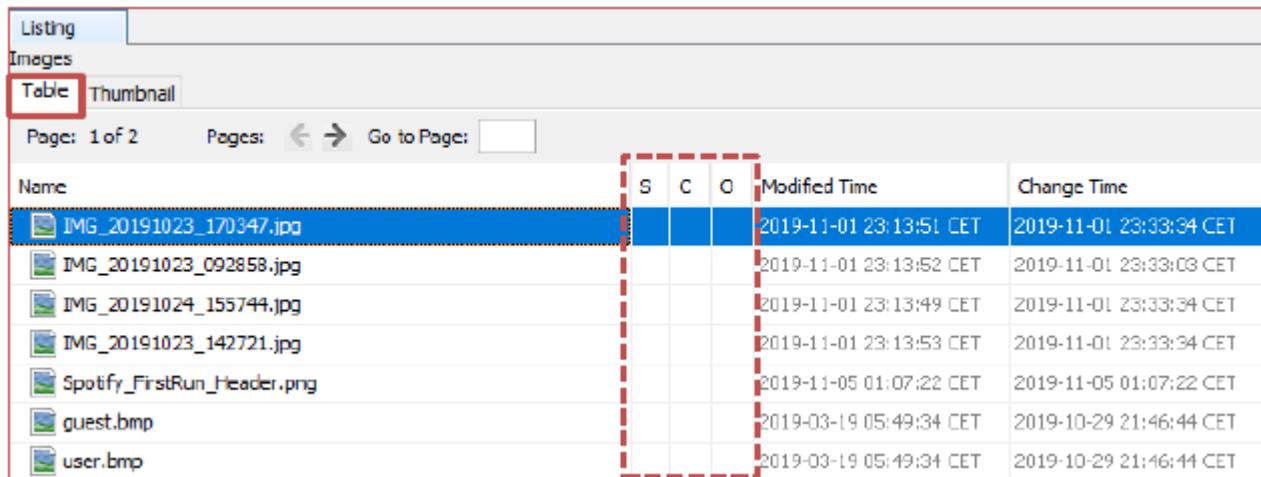
Volume:

- ▶ DOS
- ▶ GPR
- ▶ MAC
- ▶ BSD
- ▶ Solaris

File System:

- ▶ FAT
- ▶ ExFAT
- ▶ NTFS
- ▶ EXT2FS
- ▶ EXT3FS
- ▶ EXT4FS
- ▶ APFS
- ▶ HFS, HFS+
- ▶ YAFFS2

Esempio di Listing:



The screenshot shows a digital forensics tool interface with a 'Listing' tab selected. Below it, there are tabs for 'Images' and 'Table'. The 'Table' tab is currently active. At the top, there are buttons for 'Page: 1 of 2', 'Pages:', and 'Go to Page:'. A red dashed box highlights the first row of the table, which contains the file 'IMG_20191023_170347.jpg'. The table has columns for 'Name', 'S', 'C', 'O', 'Modified Time', and 'Change Time'. The data rows are as follows:

Name	S	C	O	Modified Time	Change Time
IMG_20191023_170347.jpg				2019-11-01 23:13:51 CET	2019-11-01 23:33:34 CET
IMG_20191023_092858.jpg				2019-11-01 23:13:52 CET	2019-11-01 23:33:03 CET
IMG_20191024_155744.jpg				2019-11-01 23:13:49 CET	2019-11-01 23:33:34 CET
IMG_20191023_142721.jpg				2019-11-01 23:13:53 CET	2019-11-01 23:33:34 CET
Spotify_FirstRun_Header.png				2019-11-05 01:07:22 CET	2019-11-05 01:07:22 CET
guest.bmp				2019-03-19 05:49:34 CET	2019-10-29 21:46:44 CET
user.bmp				2019-03-19 05:49:34 CET	2019-10-29 21:46:44 CET

S (score) : indica se l'elemento è di notevole importanza (notable file , con punto esclamativo) oppure se è interessante (triangolino capovolto).

C (comments) : indica se l'elemento è stato commentato, anche in un precedente caso.

O(occurrences) : indica quante volta l'elemento è stato già rinvenuto in altri reperti.

Ingest Modules :

Sono dei Plug-in responsabili di analizzare i dati presenti all'interno del file immagine:

- hashing;
- identificazione del file type;
- user activity;
- indexing;
- file carving.

Ingest Modules : Hash Lookup

Questo modulo calcola l'hash MD5 per ogni file memorizzandolo all'interno del case DB.

Hash Lookup fa una ricerca degli hash calcolati all'interno della lista di “ known hash ”.

Ogni file nel caso ha tre valore di “ known status ”:

- unknown (default);

- known (ignorable) :

Possono essere ignorati anche dagli altri moduli.

Possono essere nascosti dalla "views" area.

Possono essere nascosti dalla vista ad albero.

Velocizza notevolmente l'analisi.

- notable (known bad).

Ingest Modules : File Type

Questo modulo determina la tipologia del file analizzando la signature.

E' il modo più accurato per definire il tipo di file.

Il tipo di file viene conservato nel case DB e molti moduli dipendono da queste informazioni.

Questo modulo è basato sulla libreria *Tika* e viene impiegata la catalogazione MIME type :

- application / zip;

- audio / mpeg;

- image / jpeg.

Possono essere aggiunti ulteriori tipi attraverso la signature.

Ingest Modules : File Extension Mismatch

Per ciascun file confronta l'estensione (.doc, .jpeg) con la propria categoria e se le informazioni non sono coerenti viene etichettato.

Dipende dal modulo "file type".

Serve per trovare i file che l'utente ha provato a nascondere.

Ingest Modules : Exif parser

Questo modulo estrae i metadati Exif dai file JPEG memorizzandoli nella sezione Result.

I risultati prodotti sono :

- identificazione della fotocamera;

- identificazione del timestamp dello scatto;

- geolocalizzazione del luogo dello scatto.

Ingest Modules : Embedded File Extractor

Questo modulo estrae i file incapsulati in altri file, come ad esempio i file archivio (Zip, Rar).

I file estratti vengono salvati nel case folder, e sono visibili nella "tree view".

Vengono etichettati se protetti da password.

Ingest Modules : Email parser

Questo modulo ricerca ed analizza archivi di posta.

I risultati della ricerca sono visualizzabili nella sezione "result" nella categoria "E-Mail messages".

Gli allegati sono trattati come figli del messaggio.

I risultati sono raggruppati in *threads* ed è possibile analizzarli dettagliatamente attraverso la vista “ **Communications** ”.

Ingest Modules : Interesting Files

Questo modulo etichetta file e cartelle che si pensa essere interessanti(iPhone Backup,BitCoin wallets).

Ingest Modules : Encryption Detection

Questo modulo etichetta file e volumi che sono\potrebbero essere cifrati.

La cifratura potrebbe essere basata su :

- high entropy;
- dimensione : multiplo di 512;
- tipo di file.

Ingest Modules : Plaso

Tool open source che esegue il *parsing* di file log e altri tipi di file per estrarre i timestamp.

Estrae quanti più timestamp possibili per l’elaborazione di una timeline.

Ingest Modules : Virtual Machine Extractor

Analizza le Virtual Machine presenti all’interno del reperto :

- ricerca i file VMDK e VHD;
- crea una copia locale dei file;
- vengono inseriti in data sources.

Ingest Modules : Data Source Integrity

Calcola e valida l’hash del reperto e assicura l’integrità dell’evidence.

Recupera l’hash dei metadati del disk image o quelli inseriti dal CF.

Calcola l’hash del disk image.

Invia un alert se la validazione fallisce.

Lezione 15

L’analisi : Autopsy (seconda parte)

Ingest Modules : Recent Activity

Questo modulo estrae le attività recenti dell’utente e i risultati vengono inseriti in “Extracted Content”.:

- ◆ **Analisi dei Web Browser;**
History,cookies,download,etc.
- ◆ **Analisi dei registri;**

Dispositivi USB,Lista utenti,programmi installati,programmi eseguiti.

Analisi delle chiavi di registro mediante **RegRipper**:

- tool OpenSource
- analizza il contenuto del registro e visualizza i risultati : non è un tool

interattivo

Registri : **system,software,security,SAM,NTUSER.**

Produzione di artefatti : **dispositivi USB connessi,programmi installati ed eseguiti,informazioni di sistema e dell'utente**

- ◆ **Analisi del "cestino" (recycle bin).**

Analisi dei file cancellati ed ancora presenti nel cestino

Cambio del filename e analisi del file manifest associati ai file:

- ≥ Windows 7: \$R+[random numbers/letters] (Es.:\$R3F5245.doc)
 - < Windows 7: D+[drive letter] +[random numbers/letters]
(Es.:DC8FXD2.doc)
 - * se viene eliminata un'intera cartella solo il suo nome cambia.
-
- Analisi dei «file manifest» associati ai file:
 - \$I+[*newnamefile*]
 - Conserva l'originale *namefile* e *path*

Si ha una creazione di un **delete file** nella vista ad albero.

Ingest Modules : Keyword Search

Questo modulo genera/aggiorna un **text index** e abilita la ricerca testuale.

Si estrae ogni word da ogni file.

Se la word non esiste nell'index, viene aggiunta.

Associa la word all'ID del file.

Questo modulo utilizza :

- **Apache Solr :**
l'indice memorizzato all'interno del case folder contiene il filename, il testo estratto dal contenuto del file, il testo estratto dagli artefatti.
- **Apache Tika :**
utilizzato per l'estrazione del contenuto dei file e dei metadati.
Per file non riconosciuti o corrotti : string extractor.
- **HTML Text extractor :**
estrazione di commenti e javascript.
- **Normalizzazione**
Ricerche case insensitive.
Unicode(es. Nessuna differenza di accenti)

La ricerca si può effettuare anche per attributi (**File search by attributes** , es S C O).

Si possono cercare tutti i casi in base ad un tipo di proprietà di correlazione(files,domains,email addresses,phone numbers).

Ingest Modules : Correlation Engine

Questo modulo ricerca i file del caso all'interno del central repository e permette di correlare il caso corrente con i casi passati.

Vengono evidenziati i file/item che erano stati etichettati come notable nei casi precedenti.

Aggiorna il central repository con i file del caso corrente e permette di correlare nuovi casi al caso corrente.

Ingest Modules : PhotoRec Carver

Questo modulo permette il recupero dei file cancellati attraverso **PhotoRec** che è un tool opensource con funzione di data carving e lavora su unallocated space (lo spazio che era stato dedicato ai file che sono stati cancellati e che contiene ancora i dati relativi a quei file fin quando non viene sovrascritto attraverso il salvataggio di nuovi file).

Il risultato del recupero dei file si trovano nella vista ad albero in **\$CarvedFile**.

Ingest Modules : Android Analyzer

Questo modulo analizza i dispositivi Android attraverso il database di Android e app di terzi parti ed estrae :

- registro chiamate;
- contatti;
- messaggistica;
- browser;
- geolocation.

Viste specializzate

◆ **TimeLine Graphic Interface**

Questa vista consente di visualizzare graficamente le attività del sistema ordinate temporalmente :

- file time estratti dal file system;
- web activity estratti dal recent activity;
- exif
- plaso

◆ **Image Gallery**

Consente di visualizzare velocemente un insieme di immagini e video :

- materiale pedopornografico;
- materiale Revenge Porn;
- documenti scansionati.

Viene visualizzato il contenuto di una cartella alla volta.

◆ **Communication interface**

Visualizza i dati delle comunicazioni in due modi differenti :

- E-mail Parser;
- Android Analyzer.

E' orientato intorno agli *account* in quanto vengono visualizzate tutte le attività associate e le **relazioni** con gli altri account.

- ◆ **Geolocation**

Riepiloga tutti gli artefatti in cui sono stati estratte le informazioni sulle posizioni che sono passate per l'Exif Parser.

Che cos'è il tagging?

Il tagging permette di ritrovare facilmente il file di interesse per evidenziarlo ed esportarlo nel report.

Infatti permette di creare un riferimento ad un file di interesse per consentire di commentarlo o di etichettare una parte di un'immagine.

Essi sono associati agli esaminatori, e possono essere nascoste le etichette degli altri esaminatori.

Comments :

Attraverso i commenti si possono annotare motivi di interessi di un file.

Esso verrà visualizzato nel "Report".

Può essere salvato nel "Central Repository".

Reporting :

Generazione di un report salvato nell'apposito sezione e viene usato per esportare e condividere i risultati dell'analisi.

Può essere elaborato da ulteriori ingest module.

Tipologia di Report Modules :

- **HTML Report**

- **Portable Case:**

Versione più piccola del caso originale contenente solo i file etichettati (tagged file) e solo i file presenti nella categoria *interesting item*.

Ha un proprio database SQLite e i file sono esportati nel CaseFolder.

Extensible :

Autopsy è costituito da moduli plug-in :

- DataSource Processor
- Ingest Module
- Content viewer
- Machine Translation
- Report Module
- etc.

Linguaggio dei plug-in :

- java, **Java Module** : sono file con estensione .nbm e possono contenere più moduli

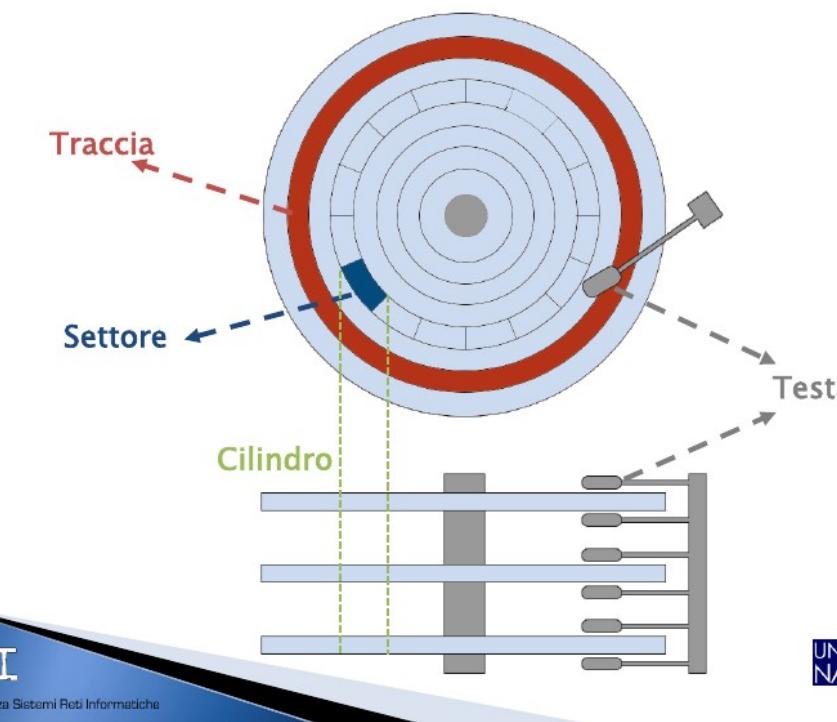
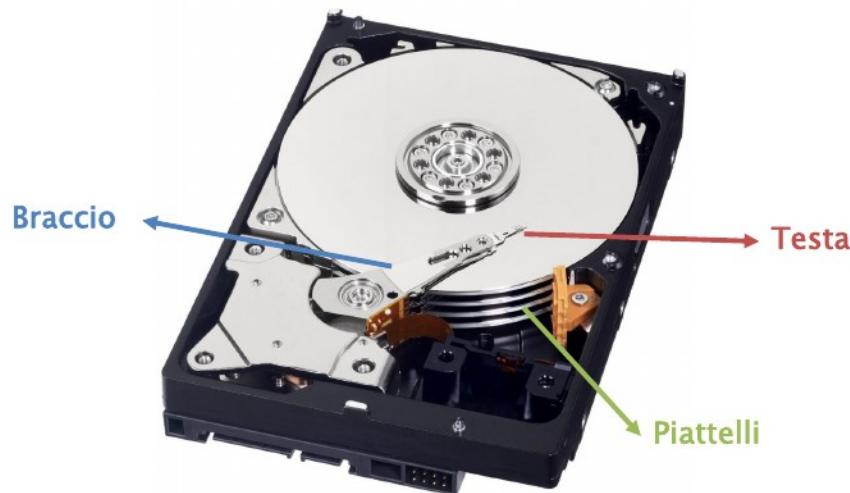
- python , **Python Module** : sono cartelle che contengono file con estensione .py e possono essere solo "Ingest Module" e "Report Module".

Copia manuale delle cartelle in una specifica directory.

Gli utenti possono creare e pubblicare dei propri plug-in.

Lezione 16 L'analisi : I volumi

L'analisi : il disco



Volume System :

Si preoccupa di gestire i volumi per :

- l'unione di più volumi in un unico grande volume
- suddivisione del volume in partizioni

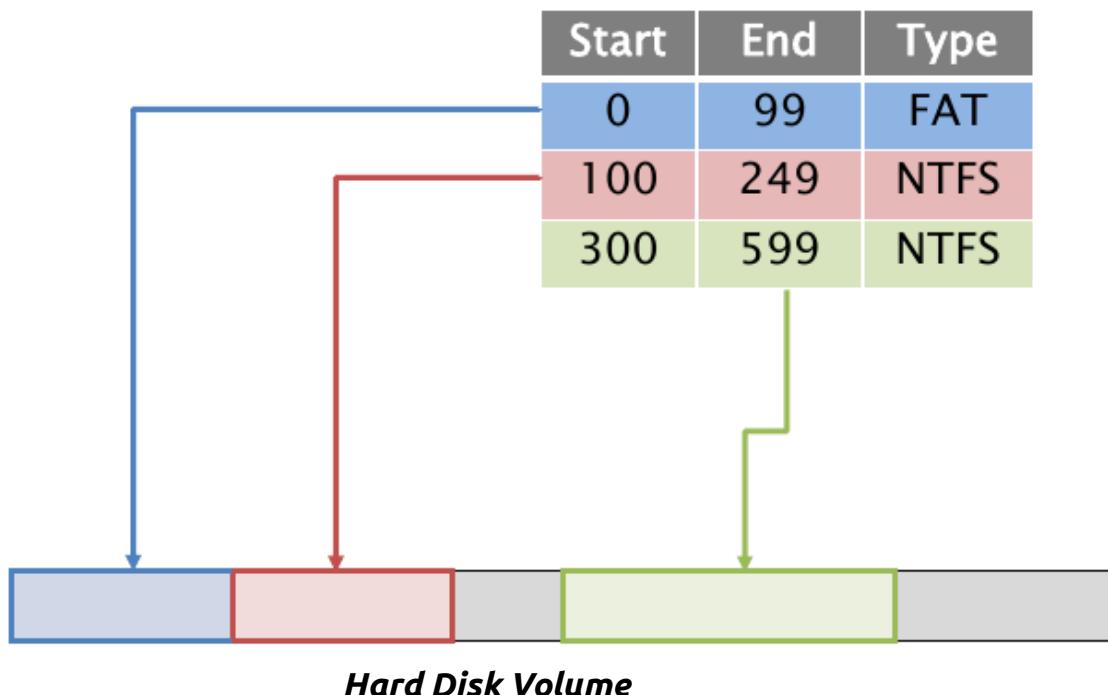
Che cos'è un volume?

Il volume è un insieme di settori per memorizzare dati.

Che cos'è una partizione?

La partizione è un insieme di settori consecutivi in un volume.

Tabella di partizione :



Indirizzamento dei settori :

- ◆ **Physical Address (LBA) :**

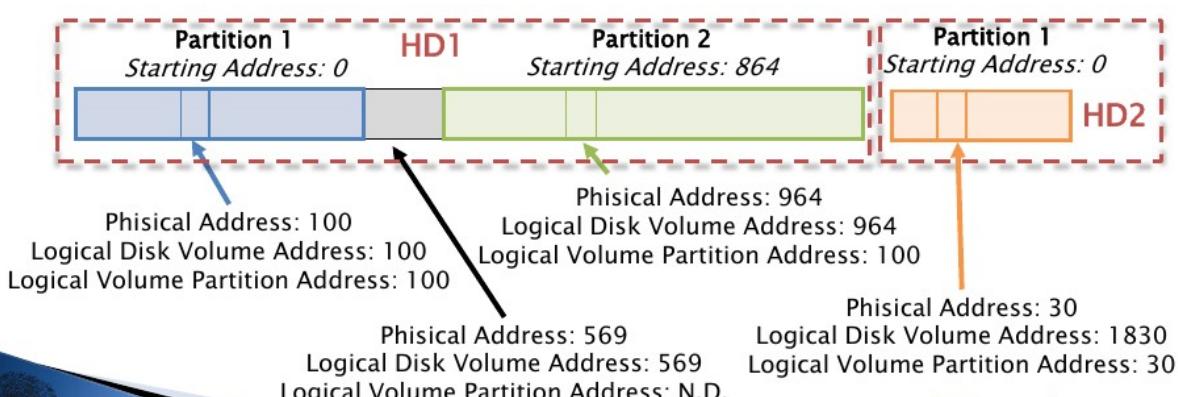
l'indirizzo del settore è calcolato in base al primo settore del disco.

- ◆ **Logical Disk Volume Address :**

l'indirizzo del settore è calcolato in base al primo settore del volume.

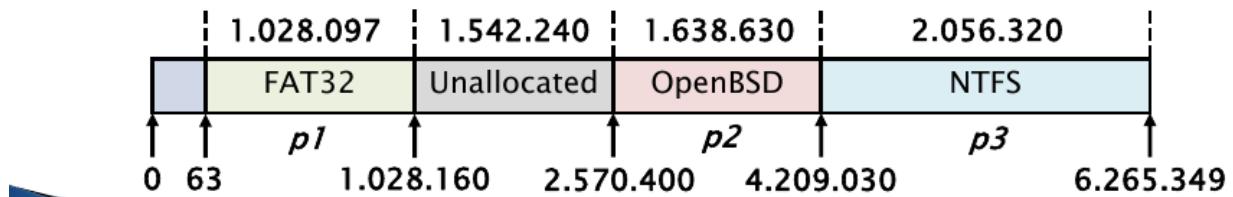
- ◆ **Logical Volume Partition Address :**

l'indirizzo del settore è calcolato in base al primo settore della partizione.



La lista delle partizioni in un file immagine :

```
root@caine:/# mm1s -t dos disk1.dd
Units are in 512-byte sectors
      Slot  Start       End       Length    Description
00: ----- 00000000000 00000000000 00000000001 Table #0
01: ----- 00000000001 00000000062 00000000062 Unallocated
02: 00:00 0000000063 0001028159 0001028097 Win95 FAT32 (0x0B)
03: ----- 0001028160 0002570399 0001542240 Unallocated
04: 00:03 0002570400 0004209029 0001638630 OpenBSD (0xA6)
05: 00:01 0004209030 0006265349 0002056320 NTFS (0x07)
```



Estrazione delle partizioni in un file immagine :

```
root@caine:/# dd if=disk1.dd of=disk1_p1.dd bs=512 skip=63 count=1028097 p1
root@caine:/# dd if=disk1.dd of=disk1_p2.dd bs=512 skip=2570400 count=1638630 p2
root@caine:/# dd if=disk1.dd of=disk1_p3.dd bs=512 skip=4209030 count=2056320 p3
```

Recupero delle partizioni in un file immagine :

```
root@caine:/# gpart -v disk2.dd
```

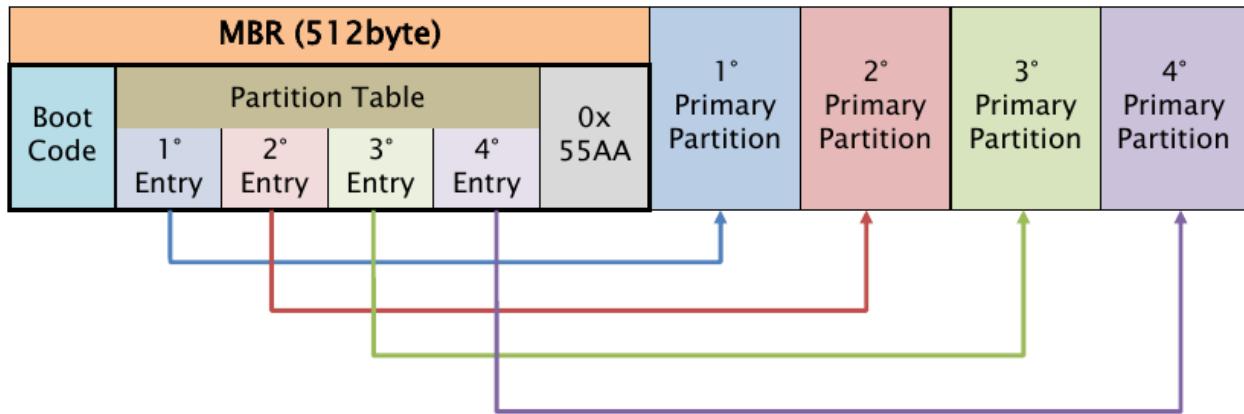
Volumi : DOS Partition

DOS Partition è il sistema di partizione più comune.

MBR (Master Boot Record) è quel settore del disco noto anche come *settore di avvio principale* composto dai primi 512 byte del disco.

E' diviso in :

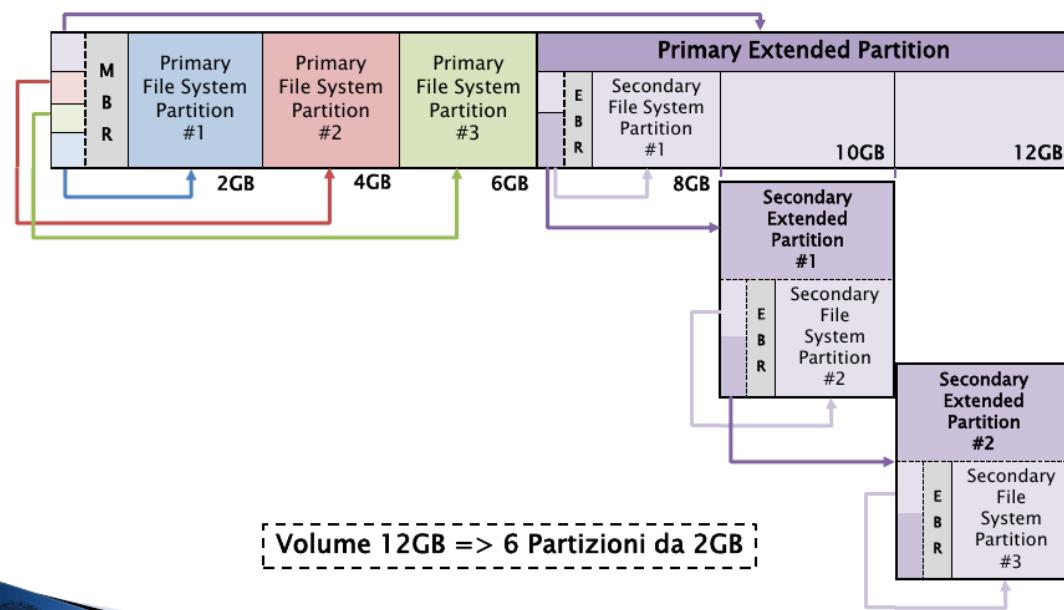
- boot code;
- partition table (max 4 entry);
 - starting CHS address;
 - ending CHS address;
 - starting LBA address;
 - number of sectors in partition;
 - type of partition;
 - flags;
- signature : 0x55AA



Primary File System Partition : partizione primaria che contiene un file system.

Primary Extendend Partition : partizione primaria che contiene altre partizioni.

- **Tabella di partizione**
- **Secondary File System Partition :** partizione secondaria che contiene un file system.
- **Secondary Extended Partition :**
 - tabella di partizione;
 - Secondary File System Partition;
 - Secondary Extended Partition;
 -



Il Boot Code è situato nei primi 446 byte del primo settore MBR.

Esempio di Boot Code : *Microsoft Boot Code* processa la tabella di partizione e ricerca ed identifica quella c.d. *bootable*, tramite il Flag.

Possibile incapsulamento di virus.

Il settore MBR viene allocato all'inizio del Disk Volume e di ogni Extended Partition, ma in questo caso si parla di **EBR(Extended Boot Record)**.

Qui non viene utilizzata la parte utilizzata al Boot Code e nemmeno due delle quattro entry della partition table.

Partition Table

Byte Range	Description	Essential
0-445	Boot Code	No
446-461	Partition Table Entry #1	Yes
462-477	Partition Table Entry #2	Yes
478-493	Partition Table Entry #3	Yes
494-509	Partition Table Entry #4	Yes
510-511	Signature value (0xAA55)	No

Byte Range	Description	Essential
0-0	Bootable Flag	No
1-3	Starting CHS Address	Yes
4-4	Partition Type	No
5-7	Ending CHS Address	Yes
8-11	Starting LBA Address	Yes
12-15	Size in Sectors	Yes

Partition Type

Type	Description
0x00	Empty
0x01	FAT12, CHS
0x04	FAT16, 16-32 MB, CHS
0x05	Microsoft Extended, CHS
0x06	FAT16, 32 MB-2GB, CHS
0x07	NTFS
0x0b	FAT32, CHS
0x0c	FAT32, LBA
0x0e	FAT16, 32 MB-2GB, LBA
0x0f	Microsoft Extended, LBA

Type	Description
0x11	Hidden FAT12, CHS
0x14	Hidden FAT16, 16-32 MB, CHS
0x16	Hidden FAT16, 32 MB-2GB, CHS
0x1b	Hidden FAT32, CHS
0x1c	Hidden FAT32, LBA
0x1e	Hidden FAT16, 32 MB-2GB, LBA
0x42	Microsoft MBR. Dynamic Disk
0x82	Solaris x86 Linux Swap
0x83	Linux
0x84	Hibernation
0x85	Linux Extended
0x86/7	NTFS Volume Set

Type	Description
0xa0/1	Hibernation
0xa5	FreeBSD
0xa6	OpenBSD
0xa8	Mac OSX
0xa9	NetBSD
0xab	Mac OSX Boot
0xb7	BSDI
0xb8	BSDI swap
0xee	EFI GPT Disk
0xef	EFI System Partition
0xfb	Vmware File System
0xfc	Vmware swap



Partition Table : analisi mediante dd

Estrazione ed analisi del primo settore MBR.
La partition table si trova a : 446-509 byte.

```
root@caine:/# dd if=disk3.dd bs=512 skip=0 count=1 | xxd
0000000: eb48 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0 .H.....
[. . .]
0000384: 0048 6172 6420 4469 736b 0052 6561 6400 .Hard Disk.Read.
0000400: 2045 7272 6f72 00bb 0100 b40e cd10 ac3c Error.....<
0000416: 0075 f4c3 0000 0000 0000 0000 0000 0000 .u.....
0000432: 0000 0000 0000 0000 0000 0000 0000 0001 .....
0000448: 0100 07fe 3f7f 3f00 0000 4160 1f00 8000 ....??.A`....
0000464: 0180 83fe 3f8c 8060 1f00 cd2f 0300 0000 ....?..`.../....
0000480: 018d 83fe 3fcc 4d90 2200 40b0 0f00 0000 ....?..M.".@....
0000496: 01cd 05fe ffff 8d40 3200 79eb 9604 55aa .....@2.y..U.
```

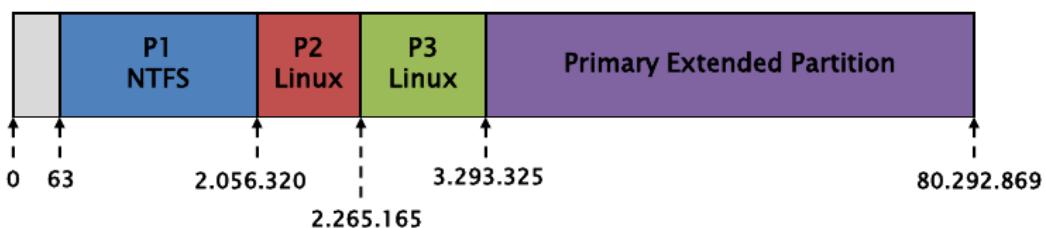
p1

p2

p3

p4

Part. 0-15	BootFlag 0-0	Start CHS 1-3	Type 4-4	End CHS 5-7	LBA 8-11	Size 12-15
P3	00	00 01 8d	83	fe 3f cc	4d 90 22 00	40 b0 0f 00
	00	8d 01 00	83	cc 3f fe	00 22 90 4d	00 0f b0 40
	00	-	Linux	-	2.265.165	1.028.160
P4	00	00 01 cd	05	fe ff ff	8d 40 32 00	79 eb 96 04
	00	cd 01 00	05	ff ff fe	00 32 40 8d	04 96 eb 79
	00	-	DOS Ext	-	3.293.325	79.999.545



Estrazione del primo settore mediante EBR

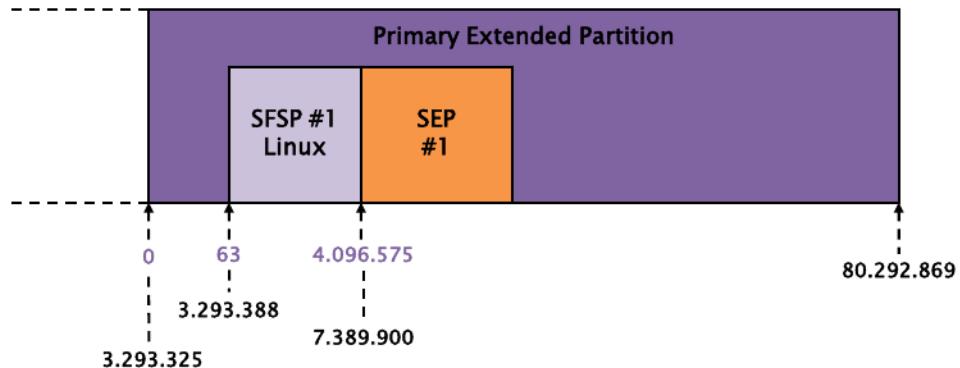
```
root@caine:/# dd if=disk3.dd bs=512 skip=3293325 count=1 | xxd
[. . .]
0000432: 0000 0000 0000 0000 0000 0000 0001 .....
0000448: 01cd 83fe 7fcf 3f00 0000 0082 3e00 0000 .....?....>...
0000464: 41cc 05fe bf0b 3f82 3e00 40b0 0f00 0000 A.....?.>.@....
0000480: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000496: 0000 0000 0000 0000 0000 0000 55aa .....U.
```

SFSP 1

SEP1

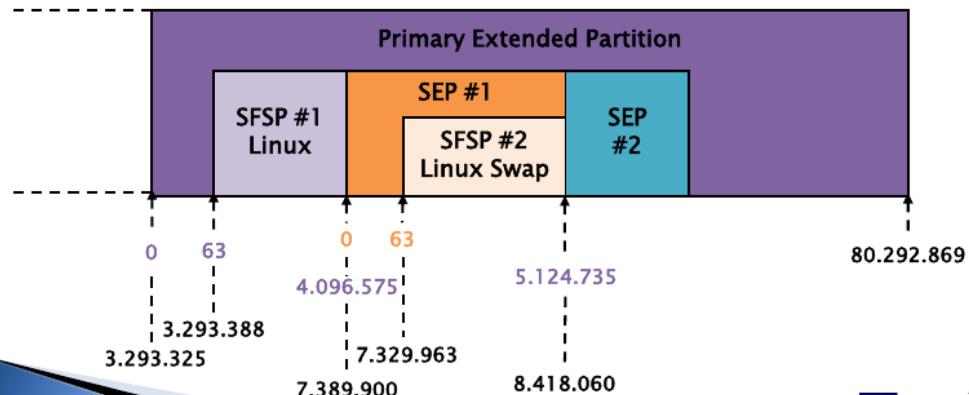
Part. 0-15	BootFlag 0-0	Start CHS 1-3	Type 4-4	End CHS 5-7	LBA 8-11	Size 12-15
SFSP #1	00	01 01 cd	83	fe 7f cb	3f 00 00 00	00 82 3e 00
	00	cd 01 01	83	cb 7f fe	00 00 00 3f	00 3e 82 00
	00	-	Linux	-	63	4.096.572
SEP #1	00	00 41 cc	05	fe bf 0b	3f 82 3e 00	40 b0 0f 00
	00	cc 41 00	05	0b bf fe	00 3e 82 3f	00 0f b0 40
	00	-	DOS E	-	4.096.575	1.028.160

Part.	Type	LBA	Size
Secondary File System Partition #1	Linux	63	4.096.572
Secondary Extended Partition #1	DOS Ext.	4.096.575	1.028.160



```
root@caine:/# dd if=disk3.dd bs=512 skip=7389900 count=1 | xxd
```

Part.	Type	LBA	Size
Secondary File System Partition #2	82 Linux Swap	63	4.096.572
Secondary Extended Partition #2	DOS Ext.	5.124.735	1.028.160



Come vedere il partizionamento mediante *fdisk -lu*

```
root@caine:/# fdisk -lu disk3.dd
Disk disk3.dd: 255 heads, 63 sectors, 0 cylinders
Units = sectors of 1 * 512 bytes
Device     Boot   Start     End   Blocks Id System
disk3.dd1          63  2056319 1028128+  7 HPFS/NTFS
disk3.dd2  *  2056320  2265164 104422+ 83 Linux
disk3.dd3    2265165  3293324  514080 83 Linux
disk3.dd4    3293325 80292869 38499772+  5 Extended
disk3.dd5    3293388  7389899  2048256 83 Linux
disk3.dd6    7389963  8418059  514048+ 82 Linux swap
disk3.dd7    8418123  9446219  514048+ 83 Linux
disk3.dd8    9446283 17639369  4096543+  7 HPFS/NTFS
disk3.dd9  17639433 48371714 15366141 83 Linux
```

Come vedere il partizionamento mediante *mmls -t dos*

```
root@caine:/# mmls -t dos disk3.dd
Disk disk3.dd: 255 heads, 63 sectors, 0 cylinders
Units are in 512-byte sectors
      Slot Start       End       Length     Description
00: ----- 00000000000 00000000000 00000000001 Table #0
01: ----- 00000000001 00000000062 00000000062 Unallocated
02: 00:00 0000000063 0002056319 0002056257 NTFS (0x07)
03: 00:01 0002056320 0002265164 0000208845 Linux (0x83)
04: 00:02 0002265165 0003293324 0001028160 Linux (0x83)
05: 00:03 0003293325 0080292869 0076999545 DOS Extended (0x05)
06: ----- 0003293325 0003293325 00000000001 Table #1
07: ----- 0003293326 0003293387 00000000062 Unallocated
08: 01:00 0003293388 0007389899 0004096512 Linux (0x83)
09: 01:01 0007389900 0008418059 0001028160 DOS Extended (0x05)
```

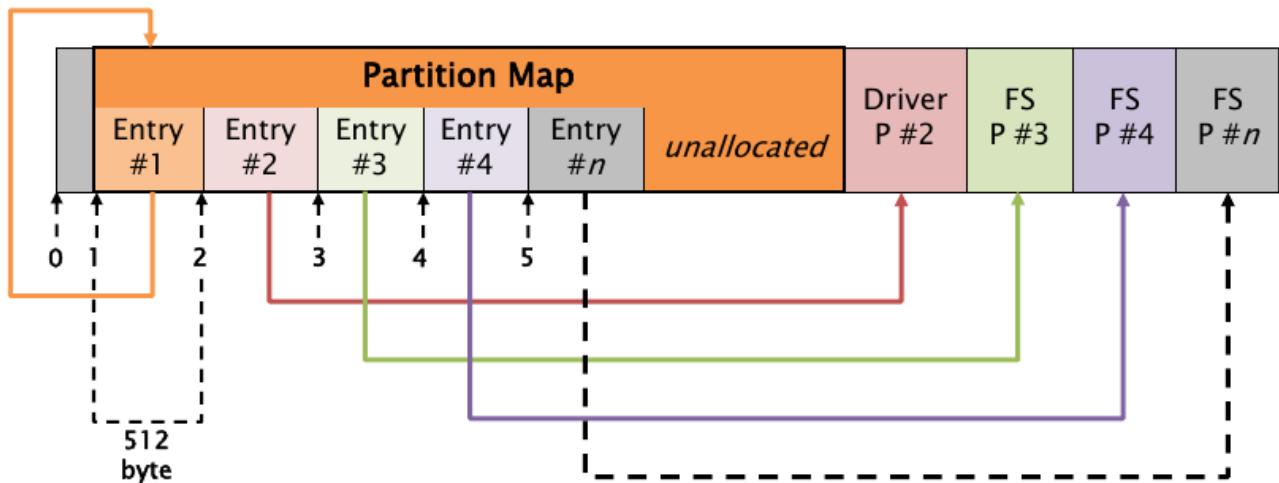
Apple Partition Map (APM)

E' una partizione impiegata soprattutto da vecchi sistemi basati su processori non Intel.

Nessun limite massimo di partizioni e gestisce volumi fino a 2TB.

La *partition map* è il secondo settore di 512 byte.

Ogni entry (512 byte) descrive una partizione e la prima entry descrive la *partition map*.



Estrazione ed analisi della prima entry (non confondere col disegno sopra)

```
root@caine:/# dd if=mac-disk.dd bs=512 skip=1 count=1 | xxd
0000000: 504d 0000 0000 000a 0000 0001 0000 003f PM.....??
00000016: 4170 706c 6500 0000 0000 0000 0000 0000 Apple.....
00000032: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000048: 4170 706c 655f 7061 7274 6974 696f 6e5f Apple_partition_
00000064: 6d61 7000 0000 0000 0000 0000 0000 0000 map.....
00000080: 0000 0000 0000 003f 0000 0000 0000 0000 .....?....
00000096: 0000 0000 0000 0000 0000 0000 0000 0000 .....[. . .]
```

Byte Range	Description	Value
0-1	Signature value	504d
4-7	Total Number of partitions	0000000a (10)
8-11	Starting sector of partition	00000001 (1)
12-15	Size of partition in sectors	0000003f
16-47	Name of partition in ASCII	Apple
48-79	Type of partition in ASCII	Apple_partition_map

Comando per visualizzare la MAC Partition Map

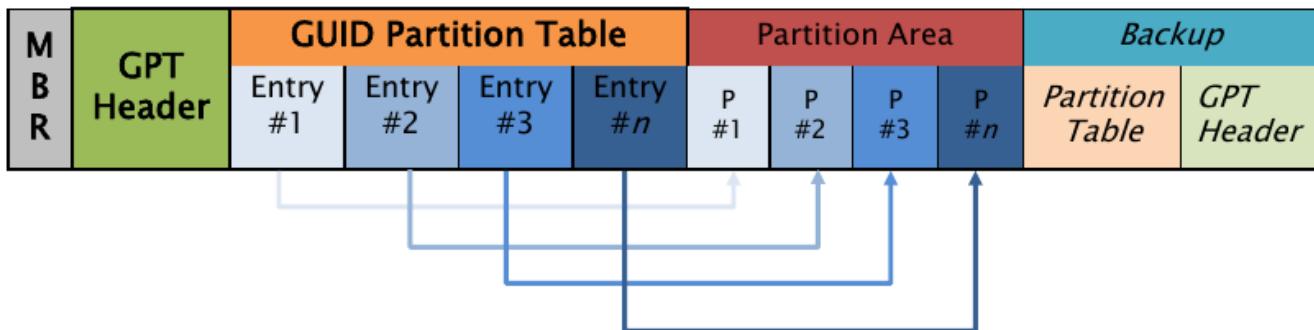
```
root@caine:/# mm1s -t mac mac-disk.dd
```

GUID Partition Table

E' un sistema di partizionamento utilizzato da EFI e si possono fare massimo 128 partizioni con volumi più grandi di 2TB.

Composto da 5 aree/sezioni :

- protective MBR : DOS Partition Table (1 settore);
- GPT Header : definisce il layout delle aree;
- Partition Table : Ogni entry descrive la partizione;
- Partition Area : locazione riservata alle partizioni;
- Backup Area : copia di Backup del GTP Header e della partition Table.



Analisi del MBR Partition Table

```
root@caine:/# mm1s -t dos gpt-disk.dd
```

GPT Header

Byte Range	Description	Essential
0–7	Signature value ("EFI PART")	No
8–11	Version	Yes
12–15	Size of GPT header in bytes	Yes
16–19	CRC32 checksum of GPT header	No
20–23	Reserved	No
24–31	LBA of current GPT header structure	No
32–39	LBA of the other GPT header structure	No
40–47	LBA of start of partition area	Yes
48–55	LBA of end of partition area	No
56–71	Disk GUID	No
72–79	LBA of the start of the partition table	Yes
80–83	Number of entries in partition table	Yes
84–87	Size of each entry in partition table	Yes
88–91	CRC32 checksum of partition table	No
92–End Sector	Reserved	No

Analisi del GPT Header

```
root@caine:/# dd if=gpt-disk.dd bs=512 skip=1 count=1 | xxd  
0000000: 4546 4920 5041 5254 0000 0100 5c00 0000 EFI PART....\...  
00000016: 8061 a3b0 0000 0000 0100 0000 0000 0000 .a.....  
00000032: 1fal 2807 0000 0000 2200 0000 0000 0000 ..(....."  
00000048: fea0 2807 0000 0000 7e5e 4da1 1102 5049 ..(.....~^M...PI  
00000064: ab2a 79a6 3ea6 3859 0200 0000 0000 0000 .*y.>.8Y.....  
00000080: 8000 0000 8000 0000 69a5 7180 0000 0000 .....i.q.....  
00000096: 0000 0000 0000 0000 0000 0000 0000 0000 .....  
[. . .]
```

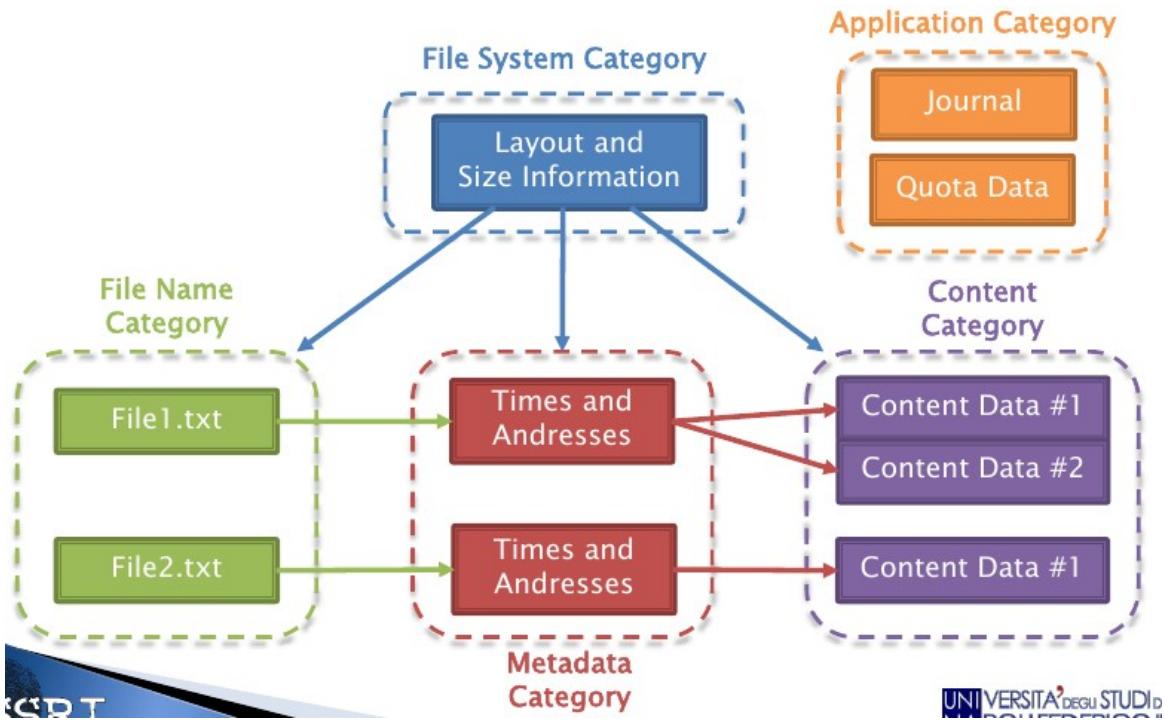
Byte Range	Description	Value
0-7	Signature value	EFI PART
12-15	Size of GPT header in bytes	5c00 (96)
32-39	LBA of the other GPT header structure	0728a1af (120.103.199)
40-47	LBA of start of partition area	0022(34)
48-55	LBA of end of partition area	0728a0fe (120.103.166)
72-79	LBA of the start of the partition table	0002 (2)
80-83	Number of entries in partition table	0080 (128)
84-87	Size of each entry in partition table	0080 (128)

Lezione 17

L'analisi : i File System (overview)

Che cos'è il file system?

Il file system è un sistema che permette la memorizzazione dei dati, organizzandoli gerarchicamente in file e in directory, in modo tale da ritrovarli velocemente.



Quali sono i dati essenziali (TRUSTED DATA) ?

Sono quei dati che se modificati/alterati causano il malfunzionamento del sistema:

- indirizzamento del contenuto del file;
- nome del file;
- dimensione del file.

Quali sono i dati non essenziali (UNTRUSTED DATA) ?

Informazioni accessorie:

- dati temporali;
- permessi utente.

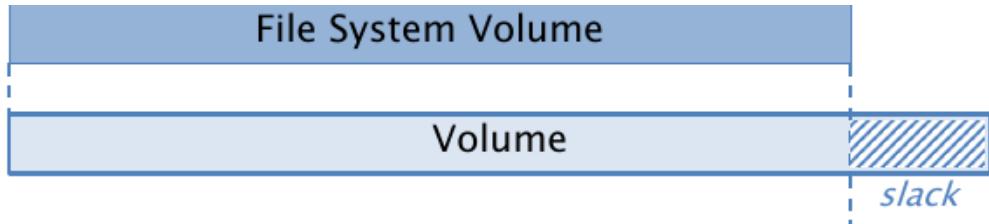
Che cos'è il file system category?

Il **file system category** contiene le informazioni generali sul file system che sono posizionate nel primo settore del volume. I dati **essenziali** sono le informazioni sul layout dei dati.

In analisi ci fornisce:

- informazioni sulla generazione del file system;
- informazioni sul layout;

- controllo di consistenza : *volume slack*

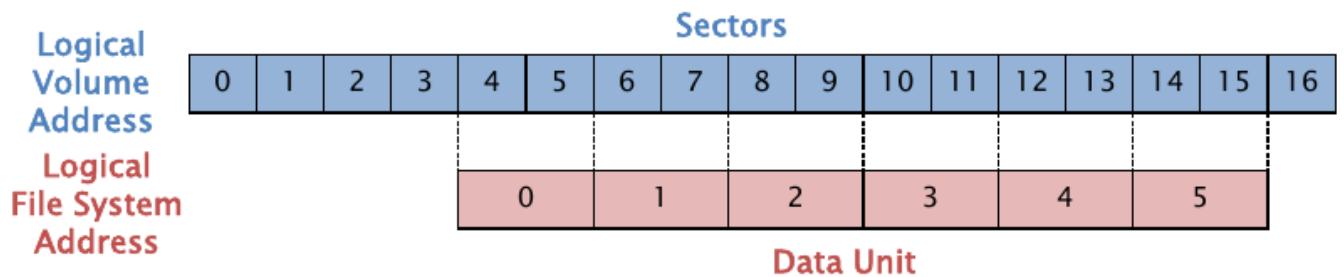


Che cos'è la *Content Category*?

Sono le locazioni di memoria impiegate per la memorizzazione del contenuto dei file:

Data Unit: raggruppamento di più settori.

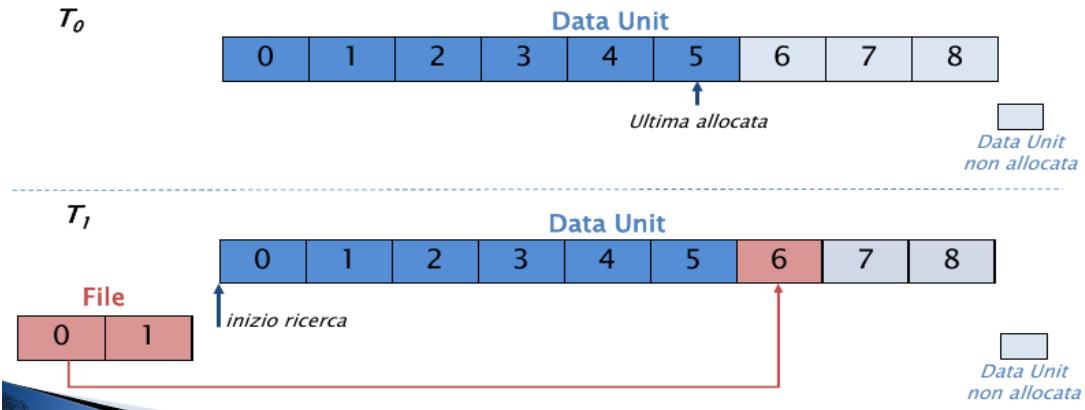
- **STATO**: allocato e non allocato.
- Logical File System address.



Le strategie di allocazione :

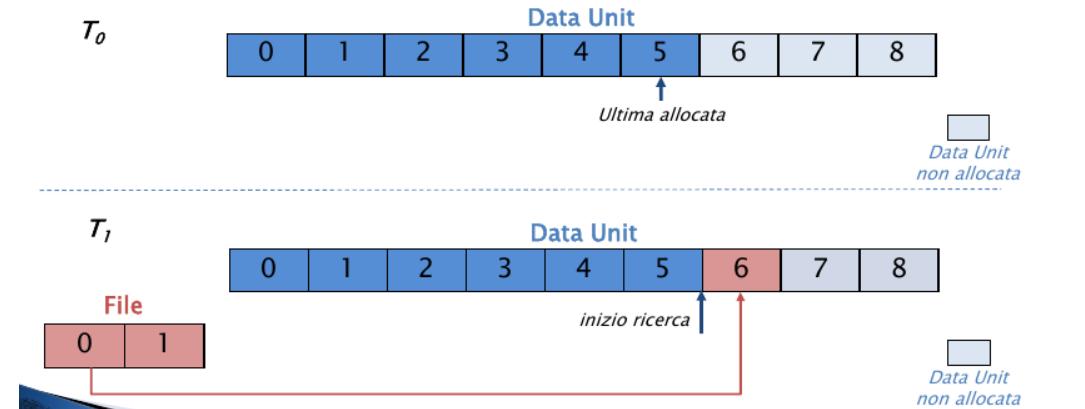
- ◆ **Strategia del primo disponibile**:

Si cerca una data unit libera ogni volta partendo dall'inizio del file system.



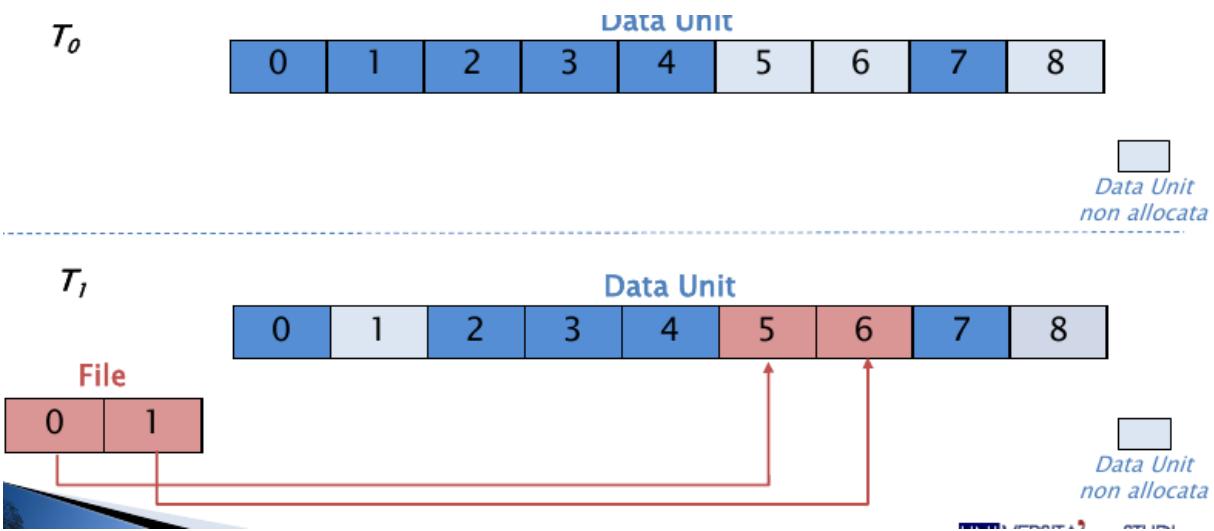
- ◆ **Strategia del prossimo disponibile**:

Si cerca una data unit libera partendo dall'ultima allocazione allocata.



◆ **Strategia del più adatto :**

Si cercando data unit libere che possano contenere consecutivamente il file.



Analisi del Content Category

- **Data Unit View :**
ricerca di settori noti del File System.
- **Logical File System Searching :**
ricerca la presenza di un contenuto specifico nei data unit.
- **Data Unit Allocation Status :**
ricerca nei data unit non allocati.
- **Consistency Check :**
ricerca di Data Unit non referenziati in *metadata category* (Orphan Data Unit).

Che cos'è la Metadata Category?

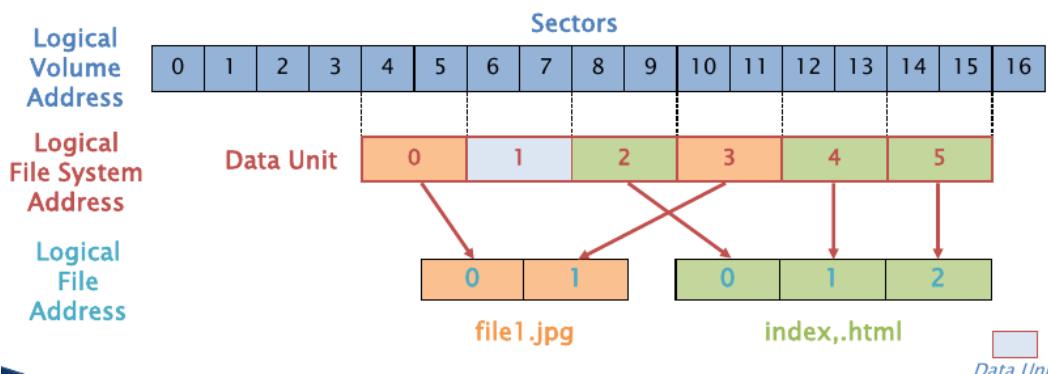
E' una categoria nella quale sono presenti le informazioni temporali dei file presenti in content category e l'indirizzo delle Data Unit allocate per il file.

In analisi ci fornisce :

- la ricerca di maggiori informazioni su di un file.
- la ricerca di file in base agli attributi descritti in questa categoria.

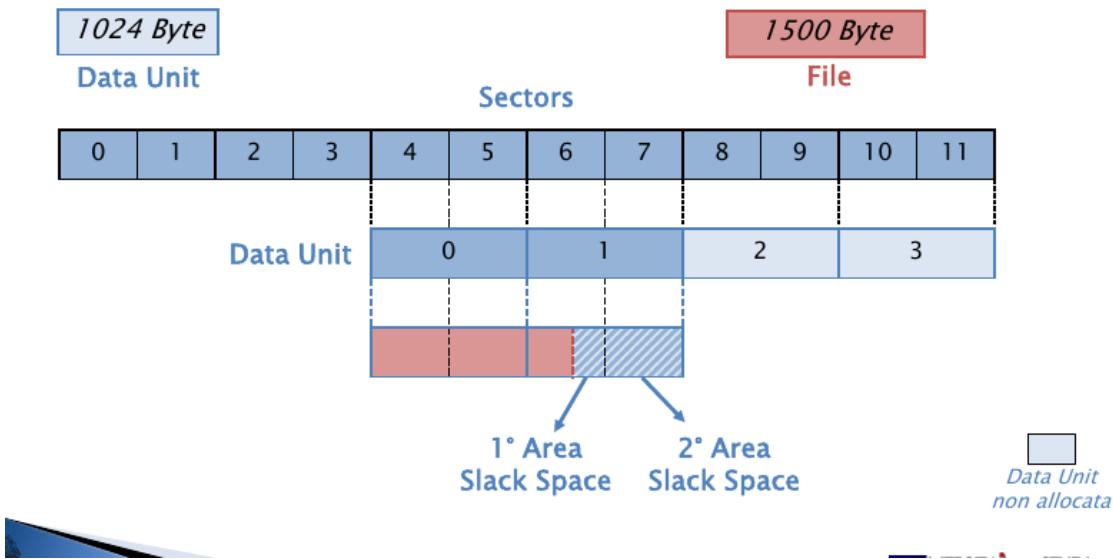
Logical File Address

E' l'indirizzo di una parte del file allocata nella data unit ed è contenuto nella data unit.



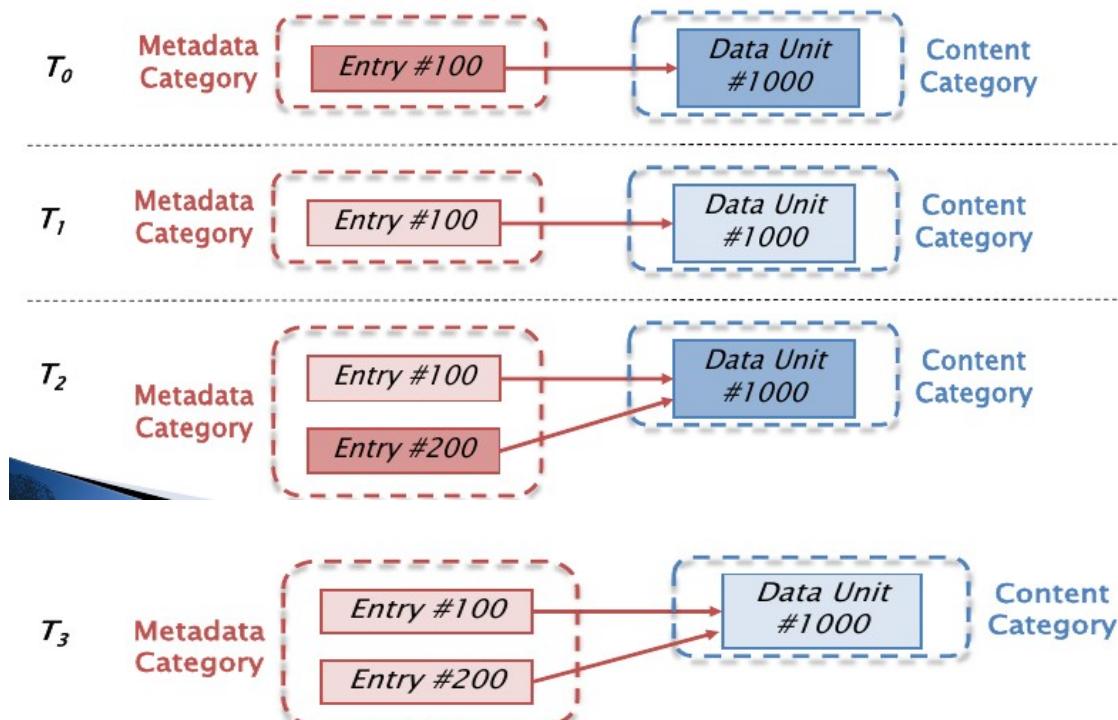
Slack Space

E' la parte non usata di una data unit allocata.



File Recovery

Recupero dei file cancellati analizzando le entry in *metadata category* con lo stato non allocato.



Compressed File

Memorizzare i dati in un formato compresso fa occupare meno spazio nella data unit.

Tre livelli di compressione :

- compressione di soli dati all'interno del file (es. jpeg , mp3)
- compressione di tutto il file : creazione di un file (es.zip,rar)
- compressione eseguita dal File System : invisibile lato applicativo e utente.

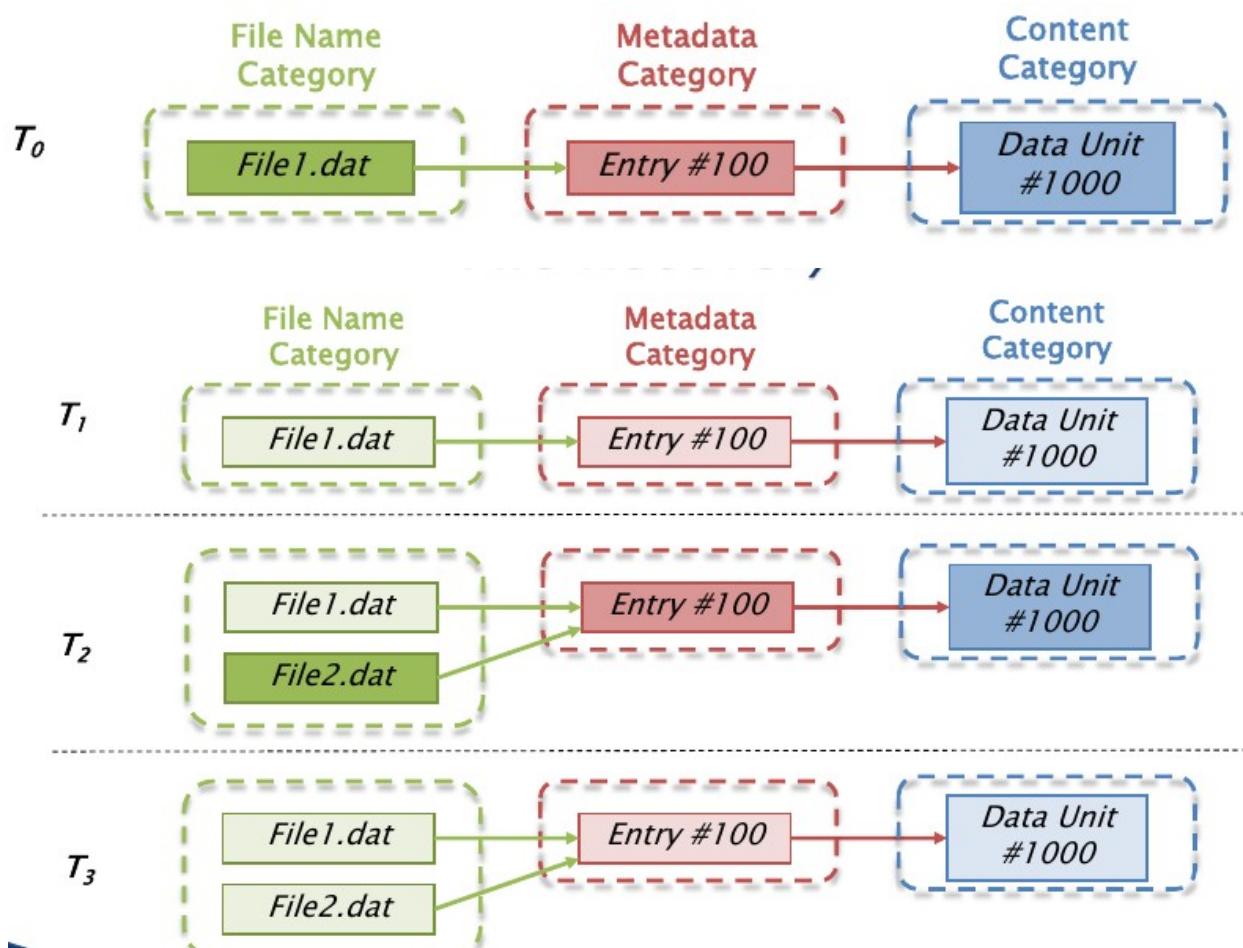
File Name Category

E' il nome assegnato a ciascun file e l'indirizzo della struttura metadato.

File Recovery:

Recupero dei file cancellati ricercando i "file name" con lo stato non allocato :

- analisi della struttura metadati indirizzata.



Che cos'è l'Application Category?

E' la categoria che comprende i file non essenziali al File System.

Journaling : conservazione delle modifiche da effettuare ed effettuate sui metadati.

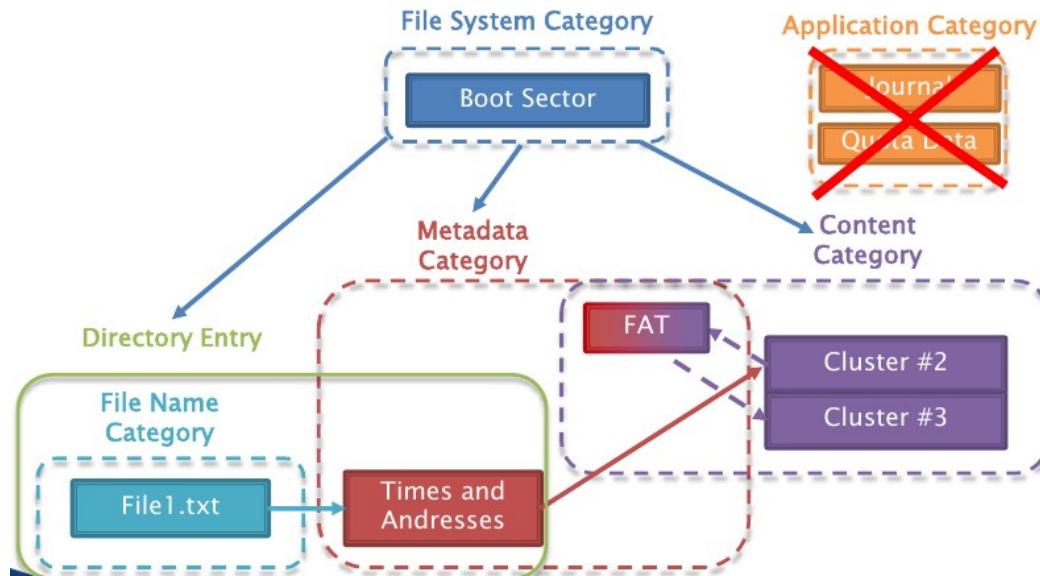
Serve per **evitare l'inconsistenza** : completamento delle operazioni di modifica e ripristino dei dati a prima delle modifiche(rollback).

In analisi serve per ricostruire eventi di un incidente recente.

Lezione 18

L'analisi : i File System (FAT)

FAT File System



FAT File System Category

Non è possibile stabilire con esattezza che tipo di file system FAT è stata utilizzato. All'interno di tale categoria però potrebbe essere presente una struttura, la FATINFO, se il file system è FAT32.

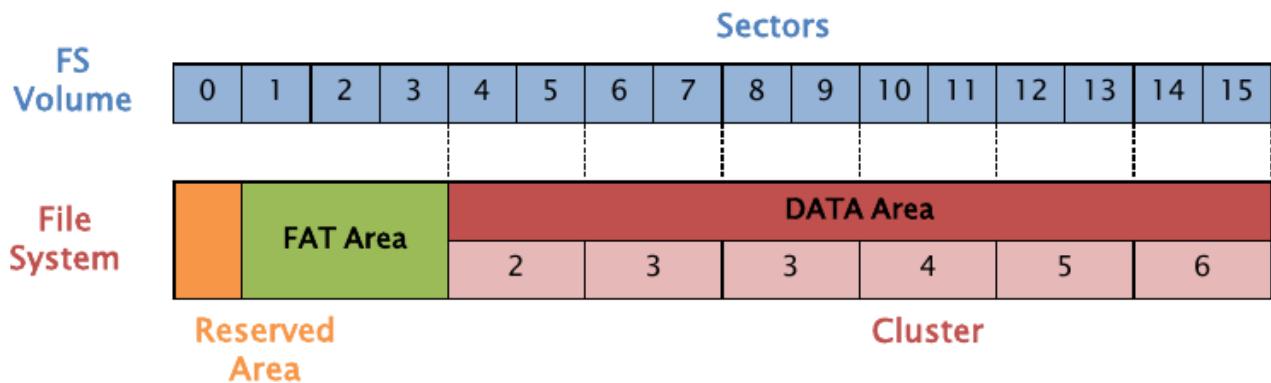
Tale struttura si trova nella Reserved Area e contiene informazioni sul numero di cluster liberi e sul prossimo cluster libero che non sono considerate essenziali.

Boot Sector : è il primo settore del file system e corrisponde alla Reserved Area. Contiene dati essenziali che sono quelli del *Physical Layout* come :

- **Reserved Area :** inizia settore 0
se è FAT 12/16 la dimensione è di 1 settore;
se è FAT 32 la dimensione è variabile.
- **Fat Area :**
dimensione size FAT x nr FAT.
- **Data Area**
dimensione = tot settori – inizio area;
dimensione Cluster;
se è FAT12/16, root directory, la quale si può trovare in qualsiasi parte della data area anche se per convenzione è il primo cluster.

Contiene dati non essenziali come :

- OEM Name : info strumento creazione del FS.
- Volume Serial Number : data di creazione (Microsoft)
- File System Label : FAT , FAT12 , FAT16 , FAT32
- FSINFO



Boot Sector

Byte	Description	Es.
0-2	Istruzioni assembly per saltare al bootcode	NO
3-10	OEM Name (ASCII)	NO
11-12	Dimensione settore (Byte)	SI
13	Dimensione Cluster (Settori) [x^2 max 32kb]	SI
14-15	Dimensione Reserved Area (Settore)	SI
16	Nr. di FAT [solitamente 2]	SI
17-18	Max nr. File in root directory [FAT12/16] [0 FAT32]	SI
19-20	Tot. settori FS [se > 65.536 => 0; usare Byte 32-35]	SI
21	Media Type [f8 - dischi fissi, f0 - disp. removibili]	NO
22-23	Dimensione FAT (settori) [FAT12/16] [0 FAT32]	SI
24-25	Nr. settori per traccia INT.13h	NO
26-27	Nr. Head dispositivo INT.13h	NO
28-31	Nr. settori prima dell'inizio della partizione	NO
32-35	Tot. settori FS [se < 65.536 => 0; usare Byte 19-20]	NO

Boot Sector (FAT12/16)

Byte	Description	Es.
36	BIOS INT.13h	NO
37	Non usato	NO
38	Extended boot signature: identifica se i successivi tre valori sono validi [29]	NO
39-42	Volume Serial Number [Windows lo genera utilizzando la data di creazione]	NO
43-53	Etichetta Volume (ASCII) [scelto dall'utente al momento della creazione del FS]	NO
54-61	File System type (ASCII) [FAT, FAT12, FAT16]	NO
62-509	Non usato [boot code]	NO
510-511	Signature [AA55]	NO

Boot Sector (FAT 32)

Byte	Description	Es.
36-39	Dimensione della FAT (settori)	SI
40-41	Nr. di FAT [se bit[7]=1 solo una delle FAT bit[0-3] è attiva, altrimenti mirror]	SI
42-43	Nr. di versione	SI
44-47	Posizione root directory (cluster)	SI
48-49	Posizione della struttura FSINFO (settori)	NO
50-51	Copia di backup del Boot Sector (settori) [6]	NO
52-63	Riservati	NO
64	BIOS INT.	NO
65	Non usato	NO
66	Extended boot signature: identifica se i successivi tre valori sono validi [29]	NO
67-70	Volume SN [Windows lo genera utilizzando la data di creazione]	NO
71-81	Etichetta Volume (ASCII)	NO
82-89	File System type (ASCII) [FAT32]	NO
90-509	Non usato [boot code]	NO
510-511	Signature [AA55]	NO

FTINFO

Byte	Description	Es.
0-3	Signature [41615252]	NO
4-483	Non usato	NO
484-487	Signature [61417272]	NO
488-491	Nr. di Cluster liberi	NO
492-495	Prossimo Cluster libero	NO
496-507	Non usato	NO
508-511	Signature [AA550000]	NO

Analisi del Boot Sector attraverso il comando *blkcat*

```
root@caine:/# blkcat -f fat fat-4.dd 0 | xxd
[...]
0000032: 4023 0300 1d03 0000 0000 0000 0200 0000 @#.....
0000048: 0100 0600 0000 0000 0000 0000 0000 0000 .....
0000064: 8000 2903 4619 4c4e 4f20 4e41 4d45 2020 ..).F.LNO NAME
0000080: 2020 4641 5433 3220 2020 33c9 8ed1 bcf4    FAT32   3....
[...]
0000496: 7274 0d0a 0000 0000 00ac cbd8 0000 55aa rt.....U.
```

Analisi di FSInfo attraverso il comando *blkcat*

```
root@caine:/# blkcat -f fat fat-4.dd 1 | xxd
[...]
0000000: 5252 6141 0000 0000 0000 0000 0000 0000 RRaA.....
0000016: 0000 0000 0000 0000 0000 0000 0000 0000 .....
[...]
0000464: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000480: 0000 0000 7272 4161 1e8e 0100 4b00 0000 ....rrAa...K...
0000496: 0000 0000 0000 0000 0000 0000 0000 55aa .....U.
```

Analisi del Boot Sector mediante *fsstat*

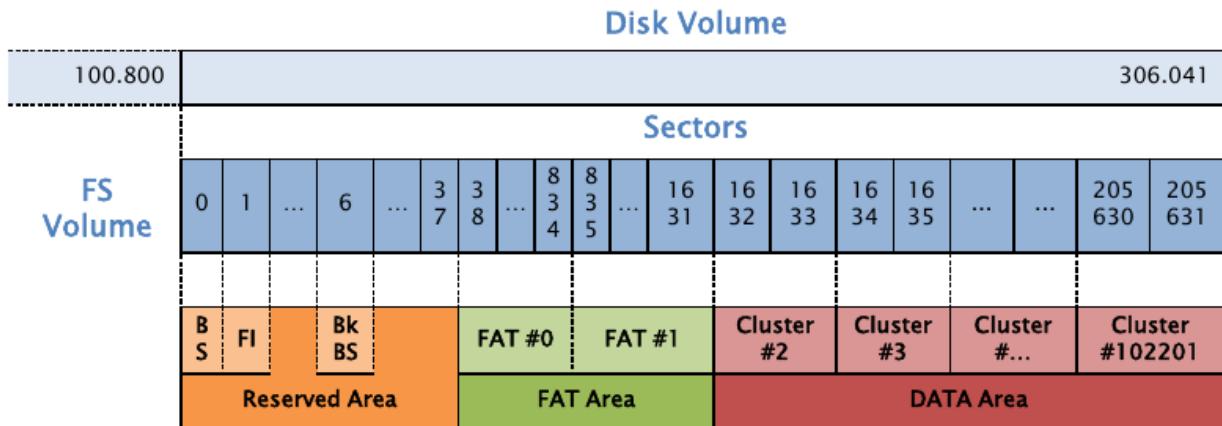
```
root@caine:/# fsstat -f fat fat-4.dd
FILE SYSTEM INFORMATION
-----
File System Type: FAT
OEM Name: MSDOS5.0
Volume ID: 0x4c194603
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): FAT DISK
File System Type Label: FAT32

Backup Boot Sector Location: 6
FS Info Sector Location: 1
Next Free Sector (FS Info): 1778
Free Sector Count (FS Info): 203836
Sectors before file system: 100800

File System Layout (in sectors)
Total Range: 0 - 205631
* Reserved: 0 - 37
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 38 - 834
* FAT 1: 835 - 1631
* Data Area: 1632 - 205631
** Cluster Area: 1632 - 205631
*** Root Directory: 1632 - 1635

CONTENT-DATA INFORMATION
-----
Sector Size: 512
Cluster Size: 1024
Total Cluster Range: 2 - 102001
[...]
```

Physical Layout FAT32



Risultati dell'analisi del *File System Category*

Si ha il recupero delle informazioni sul layout.

Controllo di possibili dati nascosti:

- bootcode;
- settori in reserved area;
- volume slack.

Confronto tra il boot sector e il backup del boot sector.

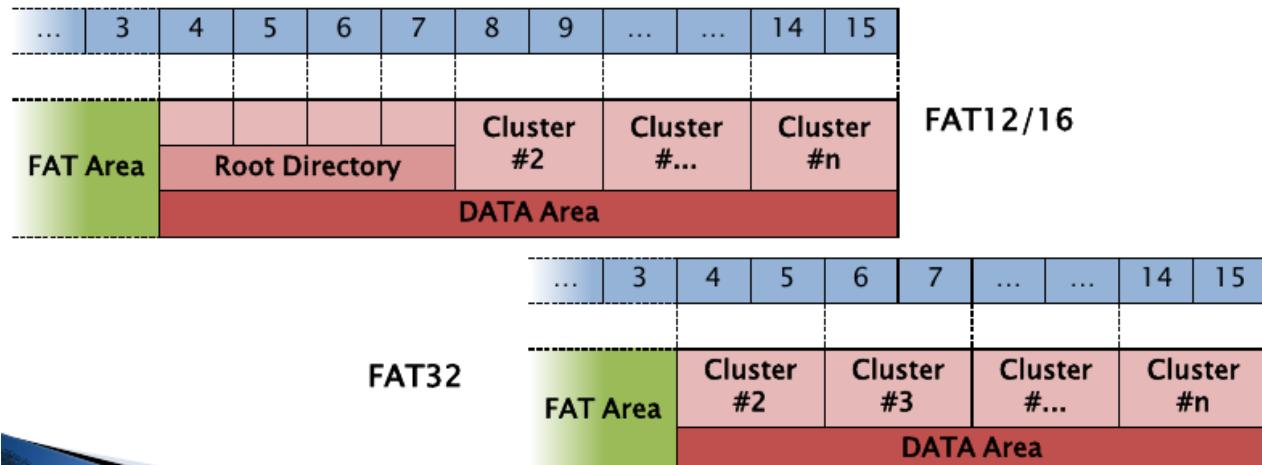
Content Category

Questa categoria contiene file e directory.

Cluster : 2 settori (max 32kb).

Primo Cluster : indirizzo 2

Solo in data area.



FAT (struttura)

Identifica lo stato di allocazione dei cluster e i successivi cluster attraverso una struttura dati definita come *Cluster Chain*.

Ad esempio se dobbiamo memorizzare un file e non lo si può memorizzare per questioni di dimensioni in un solo cluster allora diventa utile l'utilizzo della catena dei Cluster(Cluster Chain) per memorizzare il file interamente.

E' una struttura che contiene entry di ugual dimensione : FAT12 12 bit, FAT16 16bit, FAT32 32bit.

Ad ogni entry corrisponde un cluster, se quest'ultimo non è allocato l'entry è uguale a 0, se è allocato l'entry corrisponde all'indirizzo del prossimo cluster (se è l'ultimo si tratta di EOF, FAT12:0xffff, FAT16:0xffff, FAT32:0xffffffff), se è danneggiato l'entry sarà uguale a FAT12:0xff7, FAT16:0xffff7 ecc.

Indirizzamento :

La prima entry ha indirizzo 0.

L'indirizzo dell'entry è uguale all'indirizzo del cluster.

Per esempio entry[10]=cluster[10].

- entry[0] : informazione del media
- entry[1] : dirty status

Entry #	Byte	Valore
72	288-291	00000049 (73)
73	292-295	0000004a (74)
74	296-299	0000004c (76)
75	300-303	00000000 (0)
76	304-307	0000004d (77)
...
85	340-343	00000000 (0)

Conosco il cluster , come posso fare per sapere il settore?

Settore = (Cluster_Address – 2) x N_Sect_Cluster + Dim_Reserved Area + Dim_FatArea.

Dim_Reserved Area + Dim_FatArea (settore dove inizia la Data Area).

Es.: Cluster 75:

$$(75 - 2) \times 2 + \text{Sect_Cluster}_2$$

$$(75 - 2) \times 2 + 38 = 1632$$

(Dim_ReservedArea) + (Dim_FATArea) = 1632

$$(75 - 2) \times 2 + 1632 \Rightarrow 1778$$

Conoscere il settore mediante blkstat

```
root@caine:/# blkstat -f fat fat-4.dd 1778
```

```
Sector: 1778  
Not Allocated  
Cluster: 75
```

Metadata Category

Questa categoria contiene informazioni su file e directory, come ad esempio l'indirizzo del primo cluster.

Queste informazioni sono contenute nella *parent directory*, che contiene a sua volta delle **directory entry** di dimensione 32 byte. Ogni entry viene allocata per file e directory.

La parent directory è posizionata in qualsiasi parte della data area.

Serve per memorizzare il nome dei file.

File name category:

- nome file (8 caratteri) + estensione (3 caratteri)

Per nomi di file più grandi si utilizza la *long file name directory entry*.

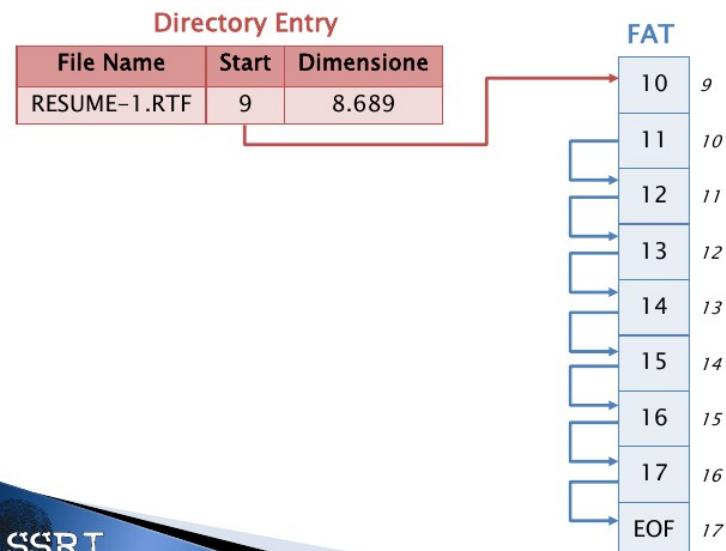
Directory entries

Byte	Description	Es.
0	Primo carattere del filename (ASCII) – 0xe5 o 0x00 [non allocato]	SI
1–10	Caratteri da 2 a 11 del filename (ASCII)	SI
11	Attributo File	SI
12	Riservato	NO
13	Ora di creazione (decimi di secondo)	NO
14–15	Ora di creazione (ora, minuti, secondi)	NO
16–17	Data di Creazione	NO
18–19	Data di Accesso	NO
20–21	Indirizzo del primo cluster (High Byte) [0 per FAT12/16]	SI
22–23	Ora di Modifica (ora, minuti, secondi)	NO
24–25	Data di Modifica	
26–27	Indirizzo del primo cluster (Low Byte)	SI
28–31	Dimensione del file [0 per le directory]	SI

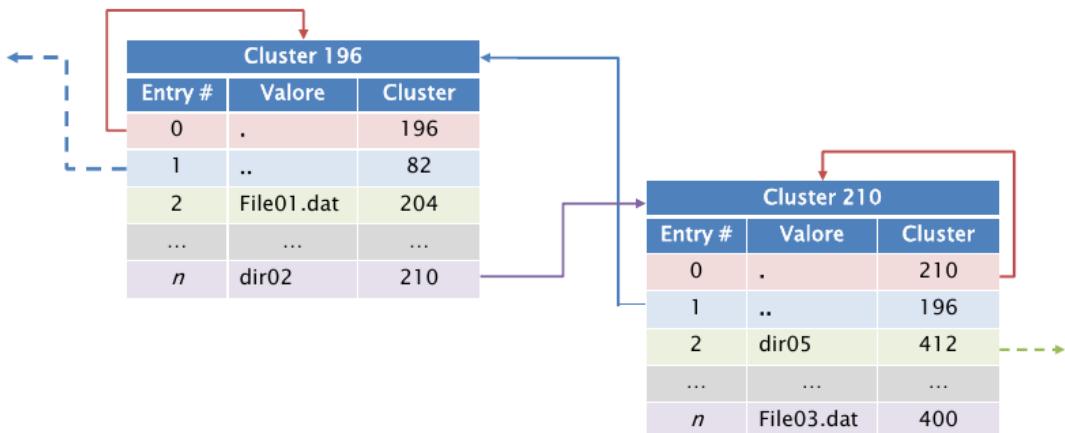
Directory entries : attributes

Flag Value bit	Description	Es.
0000 0001 (01)	Sola lettura	NO
0000 0010 (02)	File nascosto	NO
0000 0100 (04)	File di sistema	NO
0000 1000 (08)	Etichetta volume	SI
0000 1111 (0f)	Long File name	SI
0001 0000 (10)	Directory	SI
0010 0000 (20)	Archive	NO

FAT : Cluster Chain



Metadata Category : Directory



Contiene informazioni temporali (non essential data).

- Data di creazione(Windows);
- Data di modifica;
- Data di accesso;

File Name Category

Permette di mappare le strutture Metadata con un etichetta filename.

Directory entry insieme ai Metadata Category che contiene :

- filename;
- long file name directory entry* : +13 caratteri

Cluster 196		
Entry #	Valore	Cluster
0	.	196
1	..	82
2	FileSys.TXT	204
3	TextFileFAT	204
4	TE021F~1.TXT	204
...

Byte	Description	Es.
0	Nr. sequenza (bit)	SI
1-10	Nome File [caratteri da 1 a 5]	SI
11	Attributo file [0f]	SI
12	Reserved	NO
13	Checksum	SI
14-25	Nome File [caratteri da 6 a 11]	SI
26-27	Reserved	NO
28-31	Nome File [caratteri da 12 a 13]	SI

Lezione 19

L'analisi : i File System (NTFS parte 1)

Che cos'è un NTFS?

NTFS (*New Technologies File System*) è una tipologia di File System.

Ogni cosa al suo interno è un **file**:

- **\$MFT** : *Master file Table*
- **\$MFTMirr** : *backup della MFT*
- **\$Boot** : *boot sector*
- **\$Volume** : *informazioni del volume*
- **\$Bitmap** : *stato di allocazione dei cluster*
- **\$AttDef** : *definizione degli attributi*
- **\$BadClus** : *elenco dei cluster danneggiati*
- **\$Secure** : *descrittore di sicurezza*
- **\$I30** : *Index*

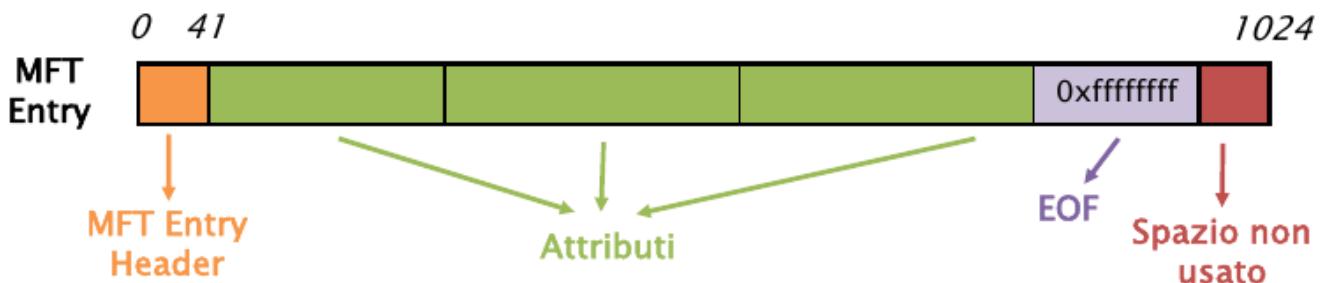
Che cos'è un Master file Table?

E' un file che contiene informazioni su *file e directory*.

Ogni *file e directory* ha almeno un entry (*File Record*) ed è grande 1024 byte(anche per il Boot Sector).

L'entry[0] corrisponde proprio alle informazioni del Master file Table.

Il Boot Sector è il cluster iniziale (*Starter Cluster*).



Master file Table (MFT Entry):

- **Dimensione** : 1024 byte
Header : 42 Byte
Attributi : strutture dati
 - **Signature** : <<File>> / <<BAAD>>
 - **Stato di allocazione** : dipende dall'attributo \$BITMAP nella entry[0] MFT.
 - **Indirizzo sequenziale**: 48 bit (File Number)
 - **Numero sequenziale**: 16 bit (contatore allocazione)
- Questi due indirizzi insieme formano il *File Reference Address*

MFT			
[...]	Nr. Seq	0003	0000 0000 0138
312	[...]	0x0003	0003 0000 0000 0138
313	[...]	0x0001	0001 0000 0000 0139
...	[...]	...	[...] ...

Tabella di byte MFT

Byte	Description	Es.
0–3	Signature (ASCII) [FILE BAAD]	NO
4–5	Offset to fixup array	YES
6–7	Number of entries in fixup array	YES
8–15	\$LogFile Sequence Number	NO
16–17	Sequence value	NO
18–19	Link count	NO
20–21	Offset to first attribute	YES
22–23	Flags [01:in use 02:directory]	YES
24–27	Used size of MFT entry	YES
28–31	Allocated size of MFT entry	YES
32–39	File reference to base record	NO
40–41	Next attribute ID	NO
42–1023	Attributes and fixup values	YES

Analisi del Master file Table (MFT) tramite *icat*

```
root@caine:/# icat -f ntfs ntfs1.dd 0-128 | xxd
0000000: 4649 4c45 3000 0300 4ba7 6401 0000 0000 FILE0...K.d.....
00000016: 0100 0100 3800 0100 b801 0000 0004 0000 ....8.....
00000032: 0000 0000 0000 0600 0000 0000 0000 .....'.
00000048: 5800 0000 0000 0000 1000 0000 6000 0000 X.....'.
[...]
00000496: 3101 b43a 0500 0000 ffff ffff 0000 5800 1.....X.
00000512: 0000 0000 0000 0000 0000 0000 0000 0000 .....'.
[...]
0001008: 0000 0000 0000 0000 0000 0000 0000 5800 .....X.
```

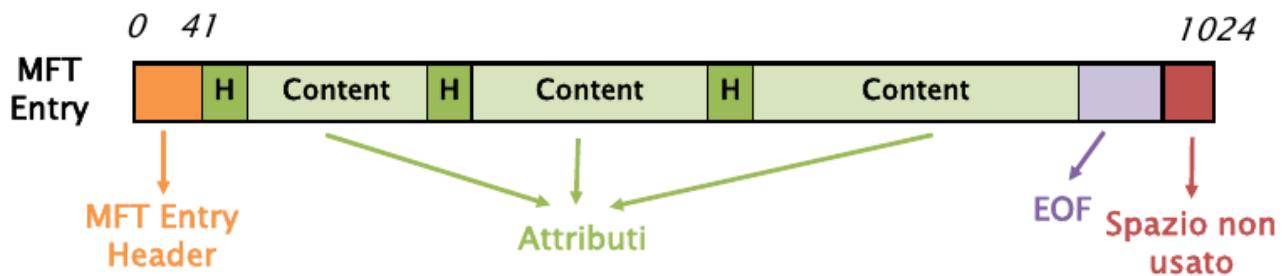
Che cos'è il *file system metadata* ?

File contenenti dati per l'amministrazione del File System.

Prime 12 entry MFT.

0	\$MFT	MFT Entry
1	\$MFTMirr	MFT Backup
2	\$LogFile	Journal
3	\$Volume	Volume Info
4	\$AttrDef	Attribute info
5	.	Root directory
6	\$Bitmap	Allocation status
7	\$Boot	Boot Sector, BootCode
8	\$BadClus	Cluster that have bad sector
9	\$Secure	Security Info
10	\$Upcase	Uppercase version of every Unicode character
11	\$Extend	Application category

Attributes



- **Attribute Header :** descrive l'attributo (tipo,dimensione,nome)
 - **ID** : identificatore univoco nell'entry (16 bit)
 - **Type ID** : identificatore tipo attributo
 - **OFFSet** del contenuto dell'attributo
- **Attribute Content :**
 - **Residente** : si trova all'interno della stessa entry
 - **Non Residente** : viene posizionato in cluster esterni.
Cluster run : cluster consecutivi

Standard Attribute Types :

Definiti nel File System Metadata attraverso **\$AttrDef**.

16 \$STANDARD_INFORMATION	<i>General information, such as flags; the last accessed, written, and created times; and the owner and security ID</i>
32 \$ATTRIBUTE_LIST	<i>List where other attributes for file can be found</i>
48 \$FILE_NAME	<i>File name, in Unicode, and the last accessed, written, and created times</i>
64 \$VOLUME_VERSION	<i>Volume information</i>
64 \$OBJECT_ID	<i>A 16-byte unique identifier for the file or directory</i>
80 \$SECURITY_DESCRIPTOR	<i>The access control and security properties of the file</i>
96 \$VOLUME_NAME	<i>Volume name</i>
112 \$VOLUME_INFORMATION	<i>File system version and other flags</i>
128 \$DATA	<i>File contents</i>
144 \$INDEX_ROOT	<i>Root node of an index tree</i>
160 \$INDEX_ALLOCATION	<i>Nodes of an index tree rooted in \$INDEX_ROOT attribute</i>
176 \$BITMAP	<i>A bitmap for the \$MFT file and for indexes</i>
192 \$SYMBOLIC_LINK	<i>Soft link information</i>
192 \$REPARSE_POINT	<i>Contains data about a reparse point</i>
208 \$EA_INFORMATION	<i>Used for backward compatibility with OS/2 applications (HPFS)</i>
224 \$EA	<i>Used for backward compatibility with OS/2 applications (HPFS)</i>
256 \$LOGGED.Utility_STREAM	<i>Contains keys and information about encrypted attributes</i>

Base MFT Entry

Quando una entry riesce a contenere/descrivere tutti gli attributi per uno specifico file.



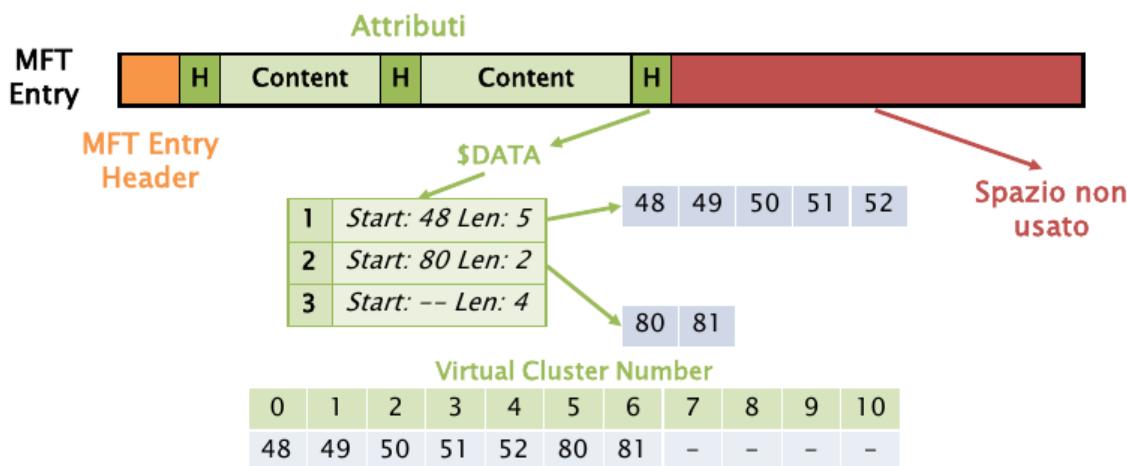
Base MFT = “è la entry principale. Contiene \$ATTRIBUTE_LIST che sarebbe la lista che ci dice dove tutti gli attributi dei file possono essere trovati.”



Non-Base MFT Entry = “è la entry dove è memorizzata l'altra parte del file”.

Sparse Attributes

Permette di risparmiare di allocare cluster ZERO (tutti 0) per l'attributo **\$DATA**.



Compressione

Vale per gli attributi non residenti e **\$DATA**.

Indicizzazione

Collezione di attributi memorizzata in maniera ordinata (*B-Tree*).

Attribute Header (*Resident Attribute*)

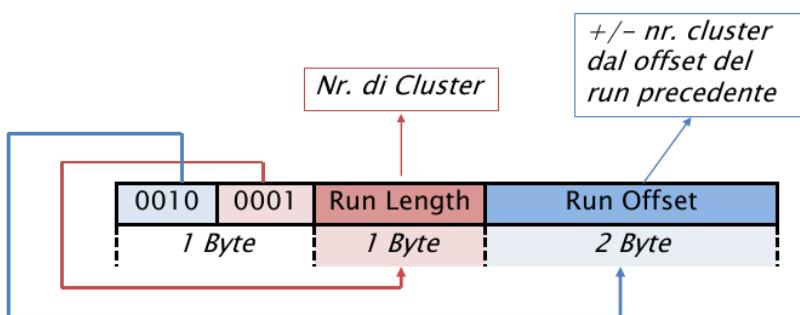
Byte	Description	Es.
0-3	Attribute type ID	YES
4-7	Length of attribute	YES
8	Non-resident flag	YES
9	Length of name	YES
10-11	Offset to name	YES
12-13	Flags	YES
14-15	Attribute identifier	YES
16-19	Size of content	YES
20-21	Offset to content	YES

Flags	
0x0001	compressed
0x4000	encrypted
0x8000	sparse

Attribute Header (*Non-Resident Attribute*)

Byte	Description	Es.
0-15	General Header	YES
16-23	Starting Virtual Cluster Number (VCN) of the runlist	YES
24-31	Ending VCN of the runlist	YES
32-33	Offset to the runlist	YES
34-35	Compression unit size	YES
36-39	Unused	NO
40-47	Allocated size of attribute content	NO
48-55	Actual size of attribute content	YES
56-63	Initialized size of attribute content	NO

Cluster Run

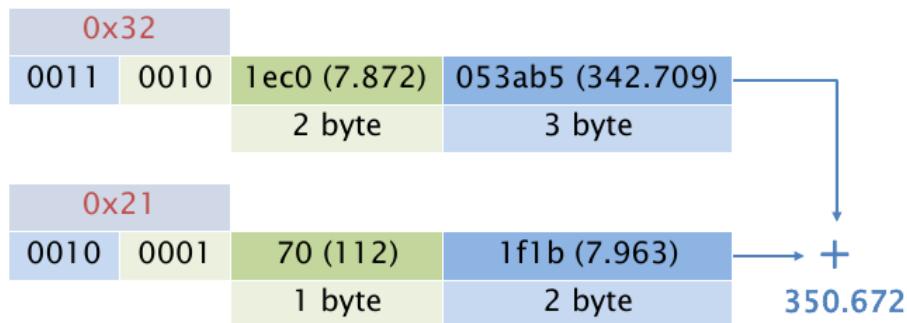


I 4 bit più significativi esprimono la grandezza in byte del campo *run offset*.
I 4 bit meno significativi esprimono la grandezza in byte del campo *run length*.

Run List

Analizzando l'Header di un attributo non residente, in questo esempio, il valore dell'offset alla runlist è il byte 64.

```
0000000: 8000 0000 6000 0000 0100 4000 0000 0100 ....`.....@....  
0000016: 0000 0000 0000 ef20 0000 0000 ..... ....  
0000032: 4000 0000 0000 0000 00c0 8300 0000 0000 @.....  
0000048: 00c0 8300 0000 0000 00c0 8300 0000 0000 .....  
0000064: 32c0 leb5 3a05 2170 1blf 2290 015f 7e31 2...:..!p..".~1  
0000080: 2076 ed00 2110 8700 00b0 6e82 4844 7e82 v...!.n.HD~.
```



File System Category

- ◆ **File System Metadata \$MFT File**

contiene la Master file Table

Cluster iniziale : Boot Sector.

Layout : da Windows 7 : cluster 786432

Corrisponde all'entry[0] di MFT.

- \$DATA : clusteri usati;
- \$BITMAP : stato di allocazione delle entry.

Analisi di MFT File mediante il comando "istat"

```
root@caine:/# istat -f ntfs ntfs1.dd 0
```

- ◆ **File System Metadata \$MFTMirr File**

E' la copia di backup della Master file Table e corrisponde alla entry[1] di MFT.

Layout : da Windows 7 : dopo il Boot Sector (16 settore)

al di sotto di Windows 7 : a metà del file system.

```
root@caine:/# istat -f ntfs ntfs1.dd 1
```

- ◆ **File System Metadata \$BootFile**

Contiene il Boot Sector:

- dimensione dei cluster;
- nr settori del File System;
- layout MFT:
- cluster iniziale;
- dimensione entry;

Corrisponde alla entry[7] di MFT.

Layout: primi 16 settori del File System.

Signature : 0xAA55

Byte	Description	Es.
0-2	Istruzioni assembly per saltare al bootcode	NO
3-10	OEM Name (ASCII)	NO
11-12	Dimensione settore (Byte)	YES
13	Dimensione Cluster (Settori)	YES
14-15	Settori riservati	NO
16-20	Non usati	NO
21	Descrizione Media	NO
22-23	Non usati	NO
24-31	Non usati	NO
32-35	Non usati	NO
36-39	Non usati	NO
40-47	Tot. settori FS	YES
48-55	Indirizzo del cluster iniziale di MFT	YES
56-63	Indirizzo del cluster iniziale di MFT Mirror	NO

Byte	Description	Es.
64	Dimensione delle entry MFT	YES
65-67	Non usati	NO
68	Dimensione dei record dell'index	YES
69-71	Non usati	NO
72-79	Serial Number	NO
80-83	Non usati	NO
84-509	Boot Code	NO
510-511	Signature (0xaa55)	NO

Analisi del Boot File mediante "istat"

```
root@caine:/# istat -f ntfs ntfs1.dd 7
```

◆ **File System Metadata \$Volume File**

Informazioni sul volume come etichetta e versione.

Corrisponde all'entry[3] di MFT.

Contiene gli attributi :

- \$VOLUME_NAME : nome in UNICODE del volume.
ID Type : 96
- \$VOLUME_INFORMATION :
 - versione di NTFS
 - dirty status
- \$DATA : 0 byte

Analisi del Volume File mediante "istat"

```
root@caine:/# istat -f ntfs ntfs1.dd 3
```

◆ **File System Metadata \$AttrDef File**

Definisce gli attributi : nomi e type id.

Corrisponde all'entry[4] di MFT.

```
root@caine:/# istat -f ntfs ntfs1.dd 4
```

Analisi del File System Category :

1) processare il primo settore del file system : boot sector;

- layout MFT;

2)processare la MFT[0] :

-\$MFTMirr.

- 3)Processare \$Volume;
- 4)Processare \$AttrDef;
- 5)Processare le altre entry MFT.

Content Category

Contenuto degli attributi :

- *residenti*: all'interno delle entry MFT
- *non residenti*: cluster esterni

Al Cluster[0] corrisponde il settore[0].

Per trovare il settore : Cluster x Settori_Cluster

- ◆ **File System Metadata \$Bitmap File**

Contiene informazioni sullo stato di allocazione dei cluster.

Bit[x] corrisponde allo stato di allocazione di un Cluster[x].

Se Bit[x] = 1 il cluster x è allocato,
se Bit[x] = 0 il cluster x non è allocato.

Corrisponde all'entry[6] di MFT.

```
root@caine:/# istrat -f ntfs ntfs1.dd 6
```

- ◆ **File System Metadata \$BadClus File**

Tiene traccia dei cluster con settori danneggiati.

Corrisponde all'entry[8] di MFT.

\$DATA = \$BAD;
-flag = Sparse;
-size = file system;

```
root@caine:/# istrat -f ntfs ntfs1.dd 8
```

- ◆ **Layout**

Esso è diverso a seconda della versione NTFS.

Zona MFT: settori consecutivi riservati per MTF.

Boot Sector : primo settore.

Dopo il boot sector si trova il File System Metadata file.

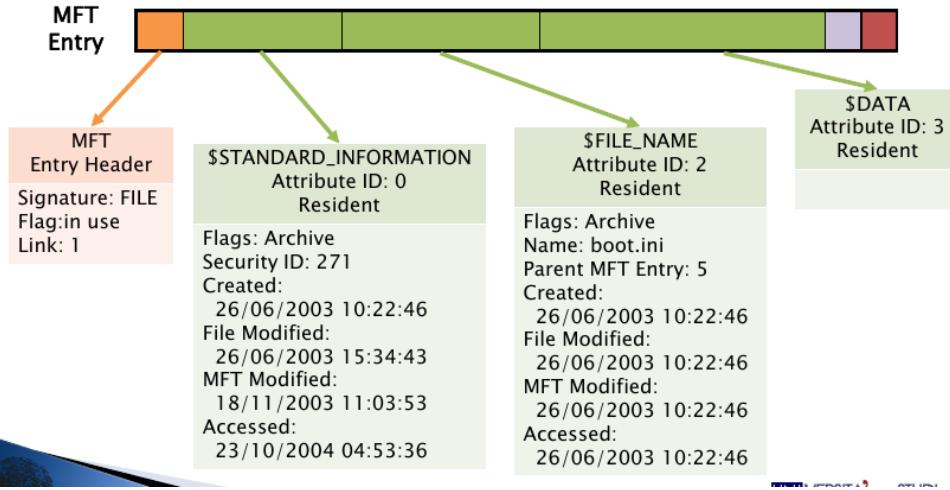
Lezione 20

L'analisi : i File System (NTFS parte 2)

Metadata Category

I metadati sono reperibili mediante gli attributi.

- Reperibili dagli attributi:



\$STANDARD_INFORMATION Attribute

Esiste per ogni file e directory.

Contiene i metadati principali come le informazioni temporali, proprietà, sicurezza e quota.

Type ID : 16.

Quest'attributo ha quattro valori temporali (timestamp) :

- data di creazione;
- data di ultima modifica;
- data di ultima modifica MFT;
- data di ultimo accesso.

\$FILE_NAME Attribute

Ogni file e directory ha almeno un attributo \$FILE_NAME.

La dimensione è 66 byte + lunghezza del nome.

Type ID : 48.

Ha il riferimento al *Parent Directory*.

\$DATA Attribute

Impiegato per memorizzare qualsiasi forma di dati : non ha formato e valori definiti. La sua dimensione può essere maggiore o uguale a 0. Se è maggiore di >700 byte si parla di attributo non residente. Type ID : 128.

Alternative Data Stream(ADS) : attributi \$DATA aggiuntivi.

\$ATTRIBUTE_LIST Attribute

Lista degli attributi nella entry.

E' utile quando un file/directory necessita di più entry per gli attributi.

Conoscendo il tipo di attributo (type ID) posso conoscere la posizione della entry che lo contiene.

Type ID : 32.

37	\$STD_INFO (ID:0)	\$ATTRIBUTE_LIST (ID:4)
		Type:16 ID:0 Entry:37
		Type:48 ID:2 Entry:48
		Type:128 ID:3 Entry:48
		Type:128 ID:3 Entry:49
		Type:128 ID:5 Entry:50

48	\$FILE_NAME (ID:2)	\$DATA (ID:3 Offset:0)
49		\$DATA (ID:3 Offset:284.201.984)
50		\$DATA (ID:5 Offset:0)

\$SECURITY_DESCRIPTOR Attribute

Describe i criteri di controllo dell'accesso che devono essere applicati a un file o una directory.

Type ID: 80.

Questo vale solo per versioni NTFS più piccole della 3.0.

File System Metadata \$Secure File

Describe i criteri di controllo dell'accesso che devono essere applicati a un file o una directory.

Corrisponde alla entry[9] di MFT :

- indice \$SDH

- indice \$SII

- attributo \$DATA (\$SDS)

Ogni file / directory contiene \$STANDARD_INFORMATION.

Questo vale solo per versioni NTFS a partire dalla 3.0.

Algoritmi di allocazione

- Allocazione delle entry**

Strategia del primo disponibile : si parte dalla entry 24.

Allocato → non allocato : cambio del flag in uso.

Non allocato → allocato : pulizia delle entry.

- Allocazione degli attributi**

-riduzione dell'ultimo attributo (\$DATA) e il marcatore EOF viene spostato in

una zona precedente.

-Crescita dell'attributo : residente → non residente e il contenuto dell'attributo prima della crescita rimane ancora nell'entry fin quando quest'ultima non richiede dello spazio per salvare un nuovo attributo.

Si possono aggiornare anche le informazioni temporali attraverso l'aggiornamento di \$FILE_NAME e \$STANDARD_INFORMATION.

Analisi del Metadata Category

1) individuazione di una entry MFT :

- individuare la MFT tramite il boot sector.

2) elaborazione del contenuto della entry :

-elaborazione degli attributi

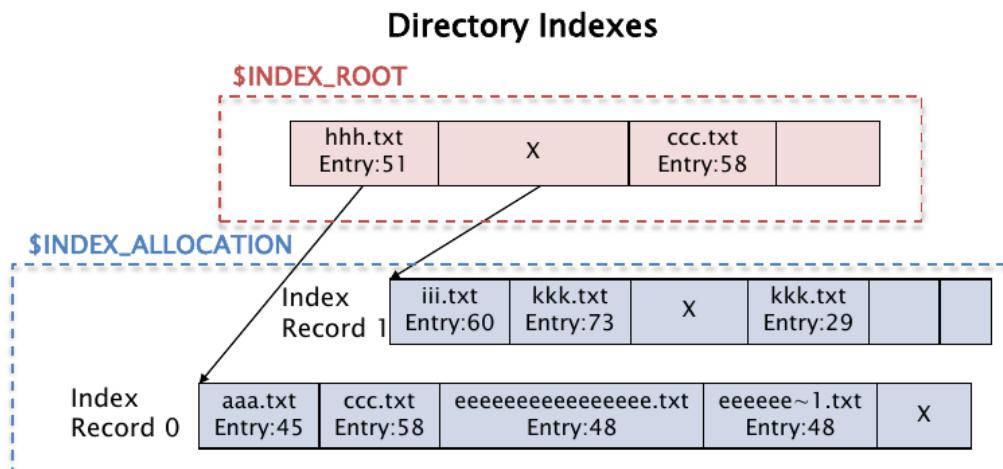
-elaborazione delle entry secondarie.

File Name Category

Ad ogni nome corrisponde un indice.

Questa correlazione viene fatta attraverso una struttura dati ordinate per chiave.

Queste strutture sono B-TREE dove i nodi sono divisi in **\$INDEX_ROOT** : radice dell'albero e **\$INDEX_ALLOCATION** : indici utilizzati.



File Name Category : Root Directory

Corrisponde all'entry[5] di MFT.

Il nome è “.”.

Risiedono tutti i “file system metadata file”.

Application Category

- **Disk Quotas (\$Quota)**

Supporto alle quote di spazio su disco :

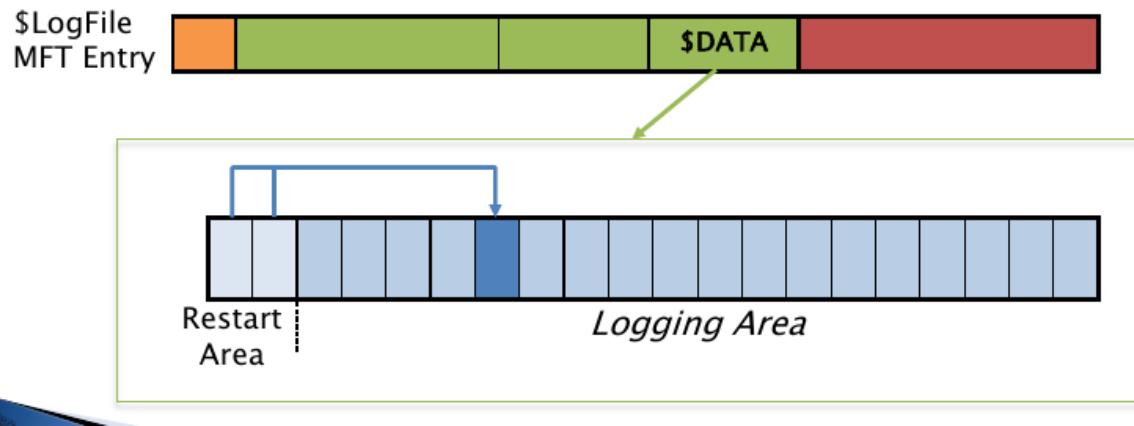
- limitare lo spazio allocato da un utente

Corrisponde alla entry[9] di MFT se il NTFS ha versione minore di 3.0.

Qualsiasi posizione di MFT se il NTFS ha versione maggiore uguale a 3.0.
Registro di Windows.

- **Logging/Journaling (\$LogFile)**

Consente di mantenere il File System in uno stato di consistenza.
Corrisponde alla entry[2] di MFT.



File Recovery

Utilizzato nel caso di eliminazione di file :

- recupero di file name eliminati dall'index directory;
- recupero entry MFT mediante attributo \$FILE_NAME;
- controllare la presenza di ulteriori \$DATA (ADS)

Lezione 21

L'analisi : i sistemi operativi

Microsoft Windows

Users

- **Account locali**
accesso al singolo sistema;
autenticazione locale.
- **Account di dominio**
accesso a tutti i sistemi attestati;
autenticazione tramite Domain Controller.
- **Account online**
accesso a tutti i sistemi attestati;
autenticazione tramite account Microsoft.

Secure Boot

Nel menu UEFI, se abilito il Secure Boot posso avviare soltanto S.O. Microsoft.

Registro di sistema

Sono le impostazioni del S.O. e dei programmi installati.

E' una struttura ad albero con cinque sotto alberi principali (**hive**) :

- **HKEY_CLASSES_ROOT**
Viene associata estensione file con l'applicazione
- **HKEY_USERS**
Impostazioni di tutti i profili utenti configurati nel sistema (**NTuser.dat**).
- **HKEY_CURRENT_USER**
Puntatore al profilo utente presente in "HKEY_USERS", loggato nel sistema.
- **HKEY_LOCAL_MACHINE**
Configurazione del computer
- **HKEY_CURRENT_CONFIG**
Puntatore alla configurazione corrente situata in "HKEY_LOCAL_MACHINE".

Ogni nodo dell'albero ha una chiave (coppia di valori : NomeChiave – Valore) e delle sottochiavi.

Tipi di chiavi	
Tipo	Descrizione
REG_SZ	NUL-terminated string
REG_EXPAND_SZ	NUL-terminated string (variabili di ambiente)
REG_BINARY	Dati binari
REG_DWORD / REG_DWORD_LITTLE_ENDIAN	4Byte (intero senza segno) [little endian]
REG_DWORD_BIG_ENDIAN	4Byte (intero senza segno) [big endian]
REG_LINK	Collegamento ad un'altra chiave
REG_MULTI_SZ	Array di NUL-terminated string

Tipi di chiavi	
Tipo	Descrizione
REG_RESOURCE_LIST	Elenco di risorse per un driver
REG_FULL_RESOURCE_DESCRIPTOR	Un descrittore di risorsa utilizzata da un driver
REG_RESOURCE_REQUIREMENTS_LIST	Un elenco requisiti delle risorse di un driver
REG_QWORD / REG_QWORD_LITTLE_ENDIAN	8Byte (intero senza segno) [little endian]
REG_NONE	Nessun tipo

Analisi del registro di sistema

- Configurazioni dell'utente.
- Dispositivi USB : pendrive,dischi esterni,etc.
- Informazioni temporali : data di ultima modifica delle chiavi.
- Strumenti per l'analisi : RegEdit(Windows),Windows Registry Recover (Mitec),Registry Viewer(Access Data).

Thumbs

Miniature di immagini presenti nelle cartelle.

Per **l'analisi di miniature** non più presenti si utilizzano *Thumbs Viewer* e *Thumbcache Viewer*.

ShellBag

Personalizzazioni utente delle visualizzazioni del contenuto delle cartelle.

BagMRU : cartella contenente lo storico di tutte le cartelle visualizzate dall'utente.

Bags : cartella contenente le impostazioni di visualizzazione delle cartelle contenute in BagMRU.

Processo di analisi nello ShellBag

Prima di tutto, si segue la lista delle cartelle presenti in MRUListex.

Successivamente si seleziona il valore della chiave relativa (nome cartella) e si segue la sottochiave della cartella.

Si visualizza la chiave MRUListex e si continua ricorsivamente la sua esplorazione.

Le informazioni che si possono ottenere da questa analisi sono :

-Bag Number

-Registry key last write time : data di primo accesso o di ultima modifica della cartella.

-Folder Name : nome della cartella

Il tool utilizzato per l'analisi è **ShellBagsView**

Event Viewer

Sistema di logging standard.

ID Evento ≥ Vista	ID Evento < Vista	Descrizione
1102	517	Log di audit cancellato
4624	528/540	Accesso di un account completato
4625	529/537	Accesso non riuscito per un account
4634	538	Un account è stato disconnesso
4674	578	Operazione eseguita con privilegi elevati
4704	608	Assegnazione di un diritto per un utente
4719	612	Cambiamento nelle politiche di audit
4720	624	Aggiunta di un nuovo account
4722	626	Un account utente è stato abilitato
4726	630	Un account utente è stato eliminato
4732	636	Un account utente è stato aggiunto ad un gruppo locale
4738	642	Un account utente è stato modificato
4739	643	Cambiamento nelle policy di dominio.

Application Data

Impostazioni dei programmi utilizzati dall'utente e file temporanei.

L'**Analisi dell'Application Data** ci fornisce il quadro complessivo dell'utilizzo del computer da parte di un utente :

- **posta elettronica;**
- **cache;**
- **cronologia;**
- **log;**
- **configurazioni;**

File Swap

Estensione della memoria volatile (RAM) rappresentata dal file *Pagefile.sys*.

Hiberfil.sys congelamento della memoria RAM in fase di sospensione/ibernazione.

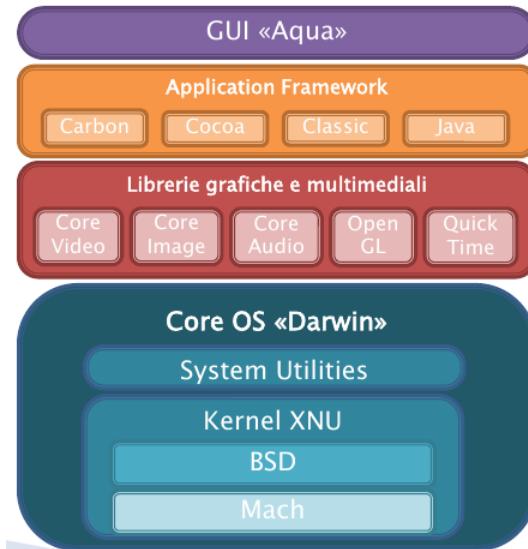
Vantaggi di Windows

- *Diffuso*
- *Documentato*
- *Supportato*

Svantaggi di Windows

- *pochi log*
- *presenza di antivirus che possono compromettere una timeline*
- *sistema commerciale*

Apple OS X/macOS



Configurazione

NetInfo è un DB ad oggetti che controlla le diverse configurazioni del S.O, le entry statiche di rete (file hosts) e definizione di tutti gli utenti.

Configurazione Server

Avviene attraverso Open Directory che è un servizio di directory e gestione di autenticazioni.

Cifratura

Per la cifratura si utilizza FileVault (cifratura della home directory, dove ci sono gran parte dei file dell'utente) o FileVault2 (per tutto il disco).

File Swap

Estensione della memoria volatile (RAM) rappresentata dal file *swapfile**.
sleepimage congelamento della memoria RAM in fase di sospensione.

Portachiavi

Accentramento delle credenziali utente.
Accesso tramite API, cifratura AES-128.
Integrazione con il servizio apple iCloud.

Analisi

Elevato numero di tecnologie proprietarie. Gli strumenti dell'analisi sono Blacklight, MacQuisition, MacForensicsLab. **Apple hdiutil**: tool da riga di comando che permette di fare copia FullDisk, copia Logica.
Si può analizzare anche la home directory utente.

Linux

E' una distribuzione basata sul kernel GNU/Linux.

Componenti:

- kernel;
- libreria di sistema;
- tool di base.

Esistono delle distribuzioni che sono *commerciali* (Fedora e CentOS) e *gratuite* (Debian e Ubuntu).

Sistema

Il sistema è multiutente e multitasking.

Struttura del file system :

Directory	Contenuto
/bin	Binari d'uso comune nel sistema.
/boot	Kernel e file necessari al boot
/dev	device fisici e logici collegati al computer
/etc	File di configurazione del sistema
/home	File degli utenti
/lib	Librerie di sistema
/mnt	Punto di montaggio per media esterni
/opt	Punto dove sono installati programmi che richiedono complesse alberature per il loro funzionamento
/root	Home directory dell'utente root

Directory	Contenuto
/sbin	Binari riservati all'uso di root
/srv	File di dati per alcuni servizi server come web e server FTP
/tmp	Locazione generale per i file temporanei
/usr	Contiene programmi non indispensabili al sistema
/usr/local	Locazione per i programmi compilati dagli utenti
/usr/src	Sorgenti del kernel e dei vari pacchetti
/var	Parte variabile dei programmi. Contiene log, mail, spool di stampa, database e quanto può essere utile a un programma da tenere in una directory scrivibile

Device /dev	Contenuto
/hda	Disco ATA master collegato al canale primario
/hdd	Disco ATA slave collegato al canale secondario
/sda	Disco SCSI con l'ID più basso collegato alla catena
/hda1	Prima partizione del disco ATA master collegato al canale primario
/loop0	Loop device. Permette visualizzare un file immagine come se fosse realmente agganciato
/eth0	Prima scheda di rete collegata al sistema
/md0	RAID software generato da Linux

Sistema di permessi di file e directory

- r : permesso di lettura;
- w : permesso di scrittura;

- x : *file* permesso di esecuzione | **directory** permesso di accesso

Utente root : nessun limite

Log

Syslog : sistema di gestione Log.

I log si trovano in : `/var/log` . I tipi di log sono : ***messages*** e ***wtmp***.

Logfinder : ricerca di tutti i file log.

Configurazioni

- in /etc si trovano le configurazioni di default come il file di configurazione di boot,l'elenco degli utenti e le password degli utenti.
- le configurazioni personalizzate si trovano in file nascosti nella home directory utente.
- le configurazioni dei programmi sono fatte con nomeprogramma.conf

Swap

Viene dedicata una partizione per l'estensione della memoria volatile:

- FAT
- 0x83 (marcatore)

Tipi di utente

- root : amministratore di sistema
- utente comune

Directory disponibili dell'utente :

- `/usr/local/bin` : file dei programmi utilizzabili dall'utente
- `/tmp` : file temporanei
- `/home/nome_utente` : directory principale dell'utente

/var

Contiene dei dati che cambiano o variano durante la normale esecuzione del sistema.Specifico per ogni sistema.

Analisi

L'analisi di un sistema linux si basa principalmente sul controllo dei percorsi `/home` , `/etc` , `/var`.

Analisi live :

- 1) `inittab/systemd` : controllare tutti i servizi eseguiti in fase di boot.
- 2) autenticazione : verificare la configurazione PAM,kerberos e openLDAP.
- 3) `\etc\fstab` : verificare il montaggio dei file system all'avvio.

Lezione 22

Mobile Forensics : acquisizione e analisi

Evidence



GSM (protocollo di comunicazione)

- **IMEI** : codice univoco del dispositivo all'interno della rete mobile.
- **SIM Card** che è formata da un nr seriale 19/20 cifre (**ICCID**) e da un identificativo nella rete mobile dell'operatore (**IMSI**).

CDMA (protocollo di comunicazione)

- **MEID** : codice univoco del dispositivo all'interno della rete mobile
- **NO SIM CARD**

Android è più diffuso di Apple IOS.

Raccolta:

1) Si disabilitano tutte le connessioni e va messo in modalità aereo.

Tutto ciò per evitare il *Remote Wipe* (pulizia da remoto) e la sovrascrittura di informazioni presenti.

2) Sbloccare il dispositivo :

per Apple si possono avere un passcode a 4 cifre oppure con 6 o più cifre.

Oppure una password alfanumerica,oppure Face ID/Touch ID. Numero di tentativi di sblocco uguale a 10.

per Android si possono avere un passcode con 4 o più cifre,Password alfanumerica,pattern,Face ID/Touch ID,Password di avvio.

Ci possono essere delle applicazioni che hanno una protezione.

Il dispositivo si può sbloccare anche attraverso le SIMCard con un PassCode a 4 cifre (PIN) e si hanno max 3 tentativi oppure con PUK di 8 cifre.

3) Spegnere il dispositivo :

Alcuni dispositivi richiedono lo sblocco.

Acquisizione

Uno degli strumenti di acquisizione utilizzato è il *Cellebrite UFED*.

Tra le periferiche da poter acquisire abbiamo le *memory card*, ad esempio MicroSD, MiniSD, etc di varie dimensioni contenente informazioni importanti come foto, video, musica, applicazioni e backup.

Le memory card sono **la prima cosa da acquisire** utilizzando un writeblock hardware/software.

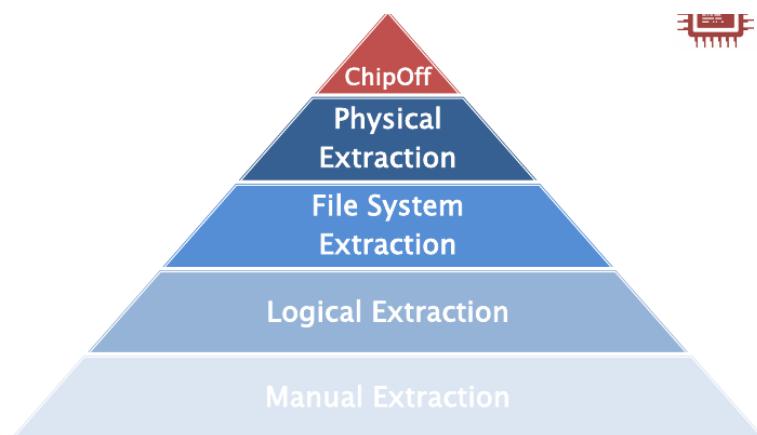
Un'altra periferica che può essere acquisita è la *SIM Card*, che può essere ad esempio Mini SIM, Macro SIM e che contiene informazioni come rubrica, sms e identificativi come : ICCID, IMSI.

Una SIM Card è strutturata nel seguente modo:

- master file(*root*);
- dedicated file(*directory*);
- elementary file(*file*).

Per acquisire il contenuto della SIM Card utilizziamo un lettore apposito.

Tipologie di acquisizione



Manual Extraction

Repertazione fotografica del contenuto che comporta l'interazione con la GUI ("scattare la foto").

Svantaggi: processo lungo, rischio modifica/cancellazione dei dati, visualizzazione limitata delle informazioni.

Limiti: display non funzionante, codice di sblocco.

Logical Extraction

Estrazione dei dati tramite API (library del dispositivo) del dispositivo.

Limiti: i risultati dipendono dall'API e quindi possono essere parziali, dunque possiamo avere solo alcune informazioni di un dato, o solo alcuni dati (nessun dato di app di terze parti). Un altro limite è il codice di sblocco.

Con l'estrazione logica possiamo scegliere la fonte di estrazione

(Device, Sim, MemoryCard) e il tipo di dati da estrarre (MMS, SMS, Musica, Audio).

File System Extraction

Estrazione dei file tramite API del dispositivo.

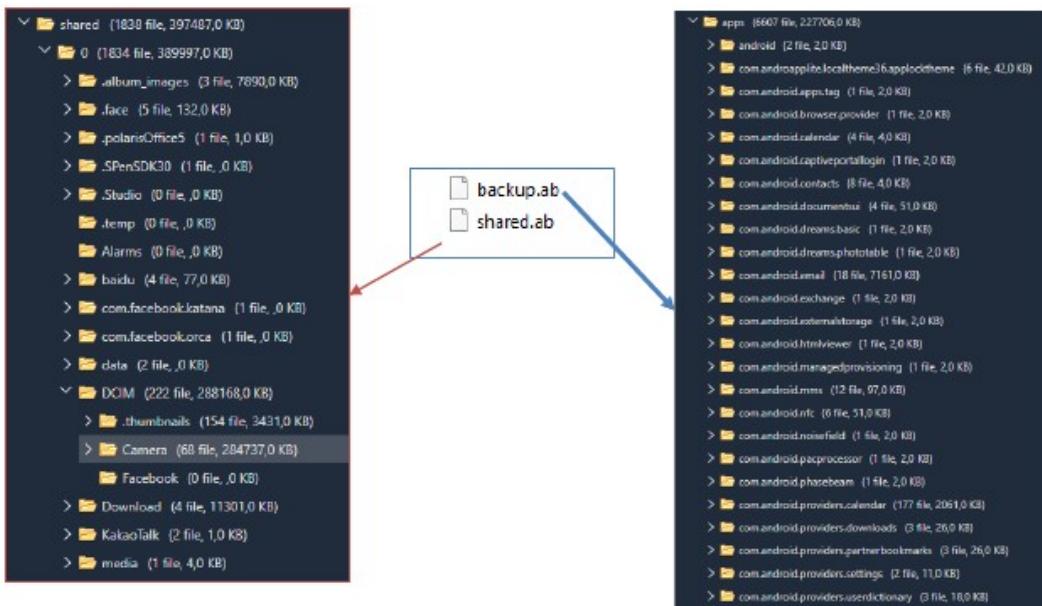
Risultato dell'estrazione: il file va processato per visualizzare i dati contenuti : i dati sono contenuti in DB SQLite.

C'è la possibilità di visualizzare i dati cancellati(entry dei DB).

Limiti: I risultati dipendono dai permessi con cui vengono fatte le richieste.

Se abbiamo un *file system completo* abbiamo a disposizione tutta la struttura della live partition.

Se invece abbiamo un *file system parziale* abbiamo a disposizione solo determinate porzioni.



Physical Extraction

Copia bit a bit della memoria del dispositivo.

Boot loader: codice immerso nella fase di avvio del dispositivo per avviare l'estrazione dei dati.

Tra le criticità si ha il bug del firmware/Chipset.

Esistono 4 metodi di Boot Loader.

Agent: tool installato nel S.O.

Advanced ADB (Android Debug Bridge)

L'output dell'estrazione va processato per visualizzare i dati contenuti.

Inoltre è possibile il recupero dei file cancellati(carving).

I limiti: produttore del dispositivo, chipset, versione del S.O., patch di sicurezza.

Chip

Estrazione fisica del chip dalla scheda madre, ma questo porta alla distruzione del dispositivo.

I limiti: dispositivo cifrato.

App

Le app estendono le funzionalità del S.O.

Esse rappresentano le principali interazioni con l'utente : produzione di dati.

Hanno un proprio dominio.

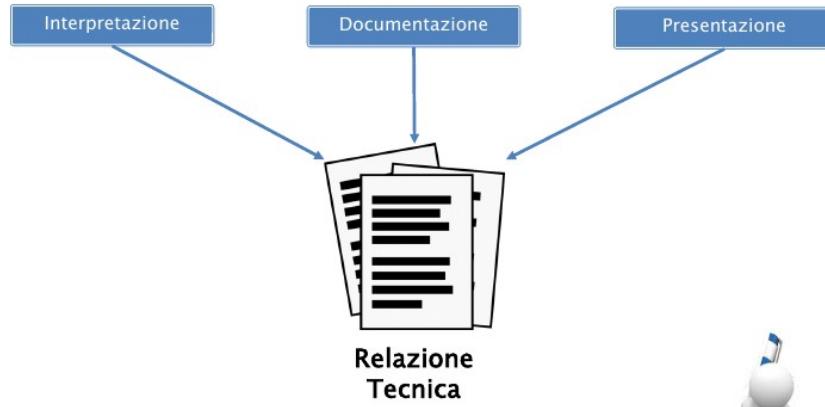
Strumenti per l'analisi

Lo strumento principale per l'analisi è ***UFED Physical Analyzer*** permette di effettuare analisi di backup ed è modulare ovvero permette di installare dei plugin aggiuntivi (per riconoscere i modelli dei dispositivi ad esempio).

Lezione 23

La fase finale : la *Relazione Tecnica*

Le fasi



La prova digitale

Contro : facilmente corruttibile.

Pro : duplicazione.

L'accertamento ripetibile

L'accertamento ripetibile deve rispettare i seguenti criteri :

- agire in modo da non alterare la prova;
- agire in modo da documentare ogni azione compiuta su di essa;
- porre la controparte in condizione di replicare quanto fatto.

La relazione tecnica

Base di partenza : *quesito*.

Descrizione dettagliata degli strumenti Hardware e Software impiegati.

Descrizione delle azioni che hanno portato / non portato risultati.

Scopo : chiunque deve poter giungere alle medesime conclusioni.

Descrizione e valutazioni

Parte descrittiva : dettagliata ed accurata attraverso documentazione fotografica.

Parte valutativa : motivazioni,descrizione dell'iter logico.

Forma di una relazione tecnica

- (1) *parte epigrafica* : indicazione degli estremi del P.P.,P.M,Giudice,descrizione dell'incarico,parti presenti ad un accertamento ,etc.
- (2) *parte descrittiva* : illustrazione degli accertamenti e/o ricostruzioni compiuti
- (3) *parte valutativa* : risposta ai quesiti con motivazione esaustiva delle conclusioni
- (4) *parte riassuntiva* : esposizione sintetica della risposta ad ogni quesito.

La forma di una relazione tecnica deve essere chiara ed intellegibile,attraverso l'utilizzo di grafici,illustrazioni e tabelle.