UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

Appunti di Computer Forensic Anno 2021

Valentino Bocchetti

Contents

1 Introduzione al corso

1.1 Contatti

N° Telefono	Email
081-19576037 (fax) 335-5456550	lorenzo.laurato@ssrilab.com info@ssrilab.com

1.2 Esame

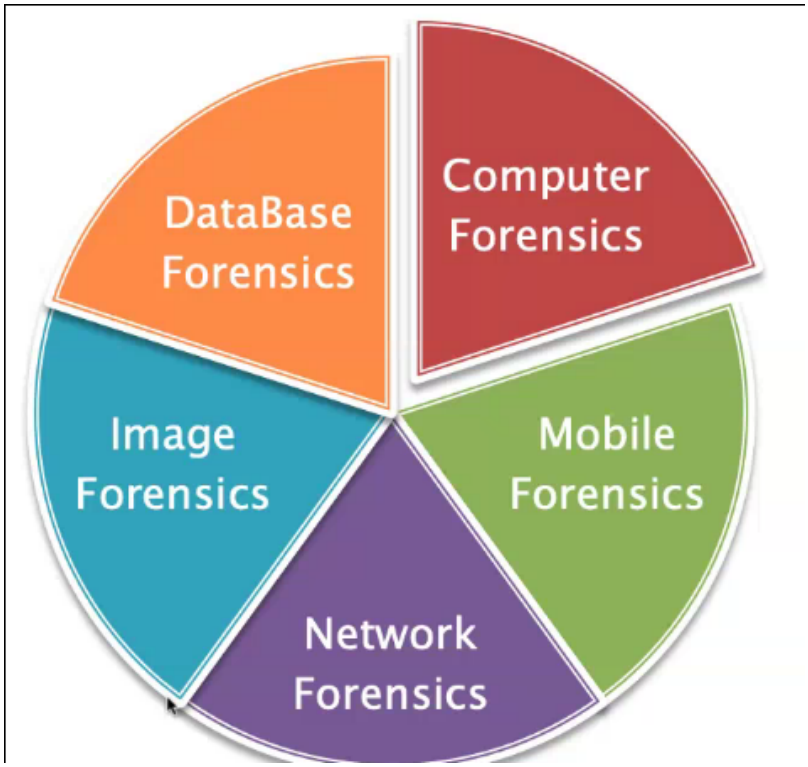
Esame scritto (risposta multipla) + orale

2 Lezione del 08-03 - Introduzione al corso

2.1 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. Il problema della Computer Forensics è il trattamento dei dati

2.2 Suddivisione della Digital Forensics



2.3 Campo di azione

Il campo di azione di un digital forenser:

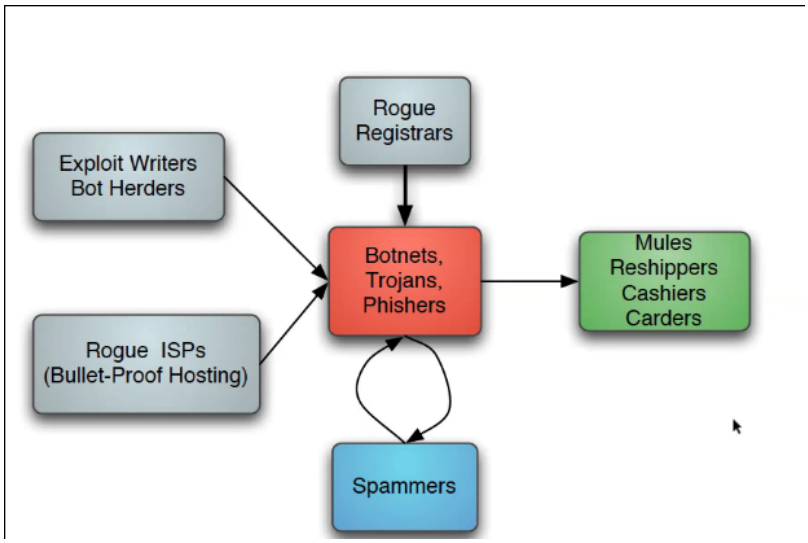
- Consulente tecnico;
- Forze dell'ordine;
- Cyber security office.

2.4 L'ecosistema del Cybercrime

Gli attacchi informatici sono implementati in varie forme diverse. La loro profittabilità dipende dal sistema che subisce l'attacco (*es* trojan, malware, etc. . .)

Esiste un mercato sulle vulnerabilità dei sistemi. Da ciò ne consegue l'interesse nella distribuzione di malware

2.5 Sistema del Cybercrime



2.6 Metodologie

- Identificazione → individuare i dispositivi che possono contenere dati rilevanti;
- Raccolta, Validazione, Preservazione → **copia forense** (copia di dati certificati tale che sia identica al dato originale);
- Analisi → entrare nel file system dei vari pc;
- Interpretazione;
- Documentazione, Presentazione → **catena di custodia**;

3 Lezione del 10-03 - Procedimento civile e penale

3.1 Il procedimento penale e civile

Area di attività del computer forenser

Area	Percentuale
Penale	48 %
Civile	20 %
Aziende	20 %
Amministrativo	7 %
Investigazioni private	5 %

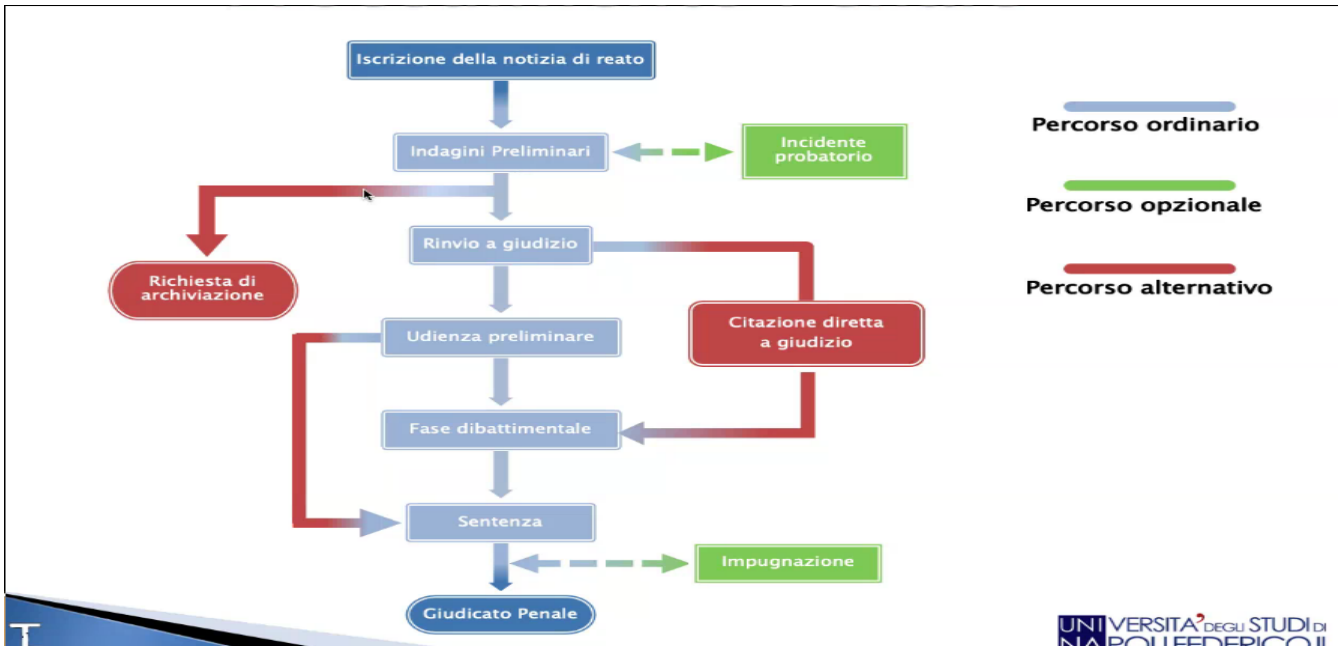
3.2 Procedimento penale

Procura della repubblica → il pubblico ministero gestisce le indagini ed ha il potere di esercitare l'azione penale.

Il tribunale → il giudice valuta le tesi accusatorie e difensive (condanna e assolve).

All'interno della procura ci sono i pubblici ministeri (lo scopo è indagare).

All'interno del tribunale ci sono i giudici.



Fase iniziale

Si svolgono le indagini ritenute necessarie alla verifica dell'attendibilità della notizia di reato (ricerca di prove). Si eseguono quindi le indagini preliminari, durante le quali si può fare uso di due strumenti giuridici:

- Perquisizione;
- Sequestro probatorio;

Entrambe atte alla conferma delle ipotesi iniziali di reato. Ne segue quindi una serie (opzionale) di **accertamenti tecnici** (richiesta di tecnici esterni).

Presente un tipo particolare di accertamento, detto **accertamento tecnico irripetibile** (provoca alterazione delle prove) $\rightarrow$ in questo caso si ha l'obbligo di avvisare entrambi le parti (indagato, parte offesa e relativi difernsori)

Misure cautelari

Sono misure emesse dal giudice atte alla limitazioni di `beni/cose` (misure reali) o limitazioni alla persona (misure personali)

Incidente probatorio

Ha lo scopo di anticipare l'acquisizione e la formazione di una prova durante le indagini preliminari

Richiesta di archiviazione

Interessa entrambe le parti e le motivazioni possibili possono essere:

- Gli elementi raccolti non sono sufficienti a sostenere l'accusa;
- L'autore del reato è rimasto ignoto;
- Il reato è estinto;
- Il fatto non è previsto dalla legge come reato;
- Il fatto è particolarmente tenue;
- La parte offesa presenta richiesta motivata di archiviazione.

Rinvio a giudizio

Avviso dell'indagato della conclusione delle indagini preliminari e informazioni sul capo di accusa

Dibattimento

Fase centrale del processo penale in cui si procede alla raccolta e acquisizione delle prove nel rispetto del contraddittorio delle parti:

- Prove documentate;
- Esame testimoniale;
- Perizia.

Sentenza

Fase conclusiva del processo penale, che può avere due risvolti:

- Proscioglimento
  - Sentenza di non doversi procedere;
  - Sentenza di assoluzione;
- Condanna;

3.3 Procedimento civile

Differenza sostanziale rispetto al procedimento penale è l'assenza nel procedimento civile della struttura della Procura (avviene tutto nel Tribunale).

4 Lezione del 15-03 - Gli attori del procedimento penale

4.1 Struttura organizzativa

- Uffici magistratura inquirente
  - Procure della repubblica `c/o` i tribunali ordinari, per i minorenni, militari;
  - Procure Generali `c/o` le Corti d'Appello;
  - Procure Generali `c/o` la Suprema corte di Cassazione;
- Uffici magistratura giudicante
  - Tribunali Ordinari;
  - Tribunali per i Minorenni;
  - Tribunali Militari;
  - Corte di Appello;
  - Suprema Corte di Cassazione.

4.2 Organizzazione della procura

Gli uffici di procura sono organizzati in gruppi di lavoro specializzati nella trattazione di specifici reati.

4.3 Pubblico Ministero (PM)

Organo dell'amministrazione giudiziaria dello stato designato per garantire il rispetto della legge e per valutare le azioni penali di un individuo. È titolare delle indagini ed ha il compito di esercitare l'azione penale.

Rappresenta la pubblica accusa.

4.4 Polizia giudiziaria

Forze di polizia che collaborano con il PM nelle attività di indagine e che dipendono direttamente dalla Procura.

Svolge determinate attività sia in modo autonomo, sia su delega dell'autorità giudiziaria:

- Attività informativa;
- Attività investigativa;
- Attività di prevenzione;
- Attività assicurativa

Ha una funzione repressiva.

4.5 La persona offesa

È il soggeto titolare del bene giuridico leso dall'autore di un reato.

4.6 Esposto, Denuncia e Querela

4.6.1 Esposto

Segnalazione all'Autorità Giudiziaria di un fatto allo scopo di far valutare se ricorre un'ipotesi di reato.

4.6.2 Denuncia

Atto con il quale si informa l'Autorità Giudiziaria di una notizia di reato perseguibile d'ufficio.

4.6.3 Querela

Dichiarazionme della persona offesa con la quale si esprime la volontà di punire il colpevole per un reato subito, non perseguibile d'ufficio. Può essere ritirata (*rimessa*) se non si tratta di reati sessuali ai danni di minori (*irrevocabile*).

4.7 Indagato e imputato

4.7.1 Indagato

La persona nei cui confronti vengono svolte indagini a seguito dell'iscrizione di un fatto a lui addebitato nel registro delle notizie di reato.

4.7.2 Imputato

La persona indagata nei confronti della quale è stta esercitata l'azione penale (rinvio a giudizio).

4.7.3 Entrambi

Hanno l'obbligo di farsi assistere da un difensore.

4.8 Avvocato

- Ruolo di assistenza;
- Ruolo di rappresentanza;

4.9 Lato giudicante

4.9.1 GIP (Giudice dell'indagine preliminare)

Funzione di garanzia dell'indagato nella fase delle indagini preliminari.

4.9.2 GUP (Giudice dell'Udienza Preliminare)

Interviene dopo l'esercizio dell'azione penale;

Giudica la richiesta di rinvio a giudizio (celebrazione del processo)

Il giudice potrà:

- Emettere decreto di rinvio a giudizio;
- Emettere sentenza di non luogo a procedere.

4.9.3 Giudice del dibattimento

Presiede a tutta la fase dibattimentale e alle relative udienze. Può essere in composizione Monocratica o Collegiale.

Per i reati più efferati è prevista una distinta composizione definita Corte d'Assise dove è presente anche la Giuria Popolare.

Emette la sentenza

4.10 Computer Forenser

Nel caso in cui siano richieste competenze tecniche può essere nominato dall'autorità giudiziaria un *consulente tecnico*.

Il CF deve impiegare metodi e strumenti che garantiscono l'inalterabilità della prova (sempre che l'ogetto in esame non porti ad un alterazione → accertamento irripetibile (c'è l'obbligo di avvisare tutte le parti))

4.10.1 Perito

Caso in cui il CF venga nominato dal Giudice.

5 Lezione del 17-03 - Genesi del diritto informatico

5.1 Reato

È quell'illecita azione o omissione teso a ledere un bene tutelato giuridicamente e a cui viene corrisposta una pena. Può essere:

- Doloso → consapevolezza e volontà di commettere un reato;
- Preterintenzionale → le conseguenze sono più gravi di quanto voluto;
- Colposo → manca la volontà di determinare un qualsiasi evento costituente reato, ma l'evento si verifica ugualmente

5.1.1 Reato informatico

Illecito che richiede conoscenze di informatica per la sua realizzazione.

Comporta il coinvolgimento di un qualunque tipo di elaboratore.

Illecito nel quale il PC interviene come strumento o come oggetto.

Ciò comporta a meglio definire il reato informatico → si rinuncia a darne una definizione precisa.

1. Lista minima e facoltativa Minima → condotte criminose che gli stati devono reprimere mediante una sanzione penale.

   Facoltativa → varia in base ai singoli paesi (condotte "solo eventualmente" da incriminare)
2. Frode informatica La frode informatica (altresì detta frode elettronica) in generale consiste nel penetrare attraverso un PC all'interno di altri PC o server che gestiscono servizi con lo scopo di rubare dati o ottenere tali servizi gratuitamente, oppure, sempre utilizzando il server al quale si è avuto accesso, clonare account di inconsapevoli utilizzatori del servizio.

5.1.2 Consiglio di Europa (2001)

Primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche (L'italia si adegua nel 2008).

5.2 Ransomware

I dati presenti sul PC sono cifrati cancellando perennemente gli originali e proteggendoli con una chiave di cifratura che l'utente non conosce e che quindi non potrà utilizzare per ripristinare i propri documenti.

Scopo → estersione (pagamento in bitcoin).

6 Lezione del 24-03 - Identificazione e Raccolta

6.1 Identificazione

Ricercare la fonte di prova che può dare una svolta alle indagini: `la prima fase è volta a individuare dove un dato è conservato`.

6.2 Preview

Consente di eseguire un'analisi di primo livello delle memorie dei dispositivi allo scopo di individuare possibili elementi di interesse investigativo.

Utilizzo di **write blocker** (`SW/HW` ad hoc). Rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova.

6.2.1 Preview DEAD

Analisi eseguita con il SO spento. → uso di write block, con il quale è possibile non alterare il dispositivo da analizzare.

HW o SW (distro linux)

PRO	CONTRO
Permette di non alterare il dispositivo	Buona conoscenza del SO e dei software da analizzare
Consente di utilizzare diversi strumenti per analizzare la memoria del dispositivo	Non sempre praticabile (sistemi embedded)

6.2.2 Preview LIVE

Analisi eseguita impiegando il SO

PRO	CONTRO
Avere una visione dell'ambiente in cui opera l'utente	Alterazione del reperto
Veloce nell'analisi dei software installati	Strumenti adeguati al sistema

6.2.3 Cambiamento di stato del dispositivo

$$\text{Acceso} \rightarrow \text{Spento}$$

$$\text{Spento} \rightarrow \text{Acceso}$$

Bisogna considerare le seguenti criticità_

- Cifratura;
- SW in esecuzione;
- Dump della RAM.

Per spegnere la il dispositivo che si vuole organizzare vanno eseguite una delle seguenti modalità:

- *unplug*
  - Potrebbe compromettere il funzionamento del SO (Server, RAID...);
- Eseguire lo spegnimento mediante il SO
  - vengono eseguite sul disco diverse operazioni.

6.3 Raccolta

Una volta identificati i dispositivi di possibile interesse investigativo si procede con il sequestro che può essere di 2 tipi:

- fisico (si prende fisicamente il supporto);
- logico (copia totale o parziale della memoria del dispositivo).

6.3.1 Catena di custodia

Uno o più documenti in cui devono essere riportati tutte le informazioni sul dispositivo che è stato sottoposto a seequestrato (fisico o logico). Contiene:

- Il luogo, data e operatore che ha reperito e collezionato la fonte di prova;
- Il luogo, data e operatore che ha esaminato la fonte di prova;
- Chi ha la responsabilità della custodia delle *digital evidences*;
- Metodo di conservazione del reperto;
- Eventuali trasperimenti di location dell'evidenza.

6.3.2 Sequestro fisico

Non sempre fattibile. È il caso di:

- Sistemi che non possono essere `fermati/spenti`;
- Sistemi distribuiti.

6.3.3 Sequestro logico

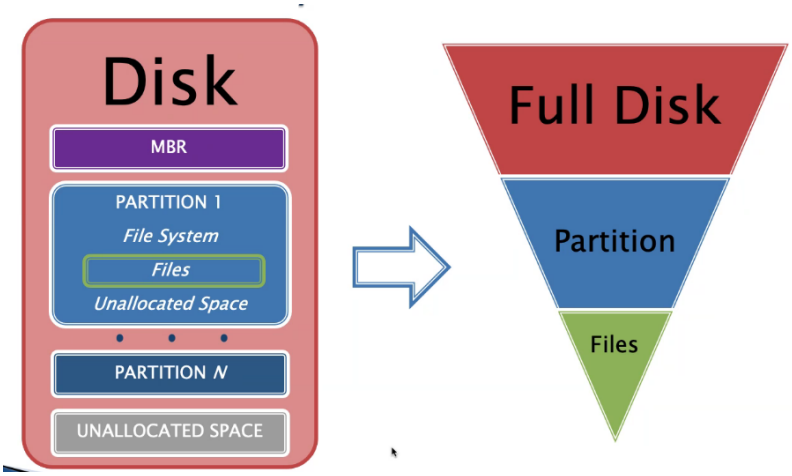
Duplicazione dei dati di *possibile* interesse investigativo (copia forense).

6.4 Copia forense

Garanzia di ripetibilità dei successivi accertamenti che verranno eseguiti sulla copia forense

Rispetto alla comune copia, questa risponde a:

- Validazione;
- Copia;
- Preservazione.



6.4.1 Acquisizione fisica

Copia *bit a bit* dell'intero supporto di memoria: dati e qualsiasi informazione sulla gestione dei dati (tabella partizioni, MBR, meta dati del file system). Due tipi di sistemi:

- Clonazione
  - ha come risultato un supporto pressochè a quello originale;
  - facilmente alterabile;
  - utilizzato solo in casi particolari (bisogna analizzare il supporto reinserendolo all'interno del proprio habitat)
- File Immagine
  - Rappresentazione del supporto originale sottoforma di file.

6.4.2 Strumenti

Di tipo o HW o SW

7 Lezione del 29-03 - Fasi del trattamento (validazione e preservazione)

7.1 Hash

L'algoritmo restituisce una stringa a lunghezza fissa di esadecimale apartire 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 è invertibile, ossia non è possibile ricostruire il dato originale a partire dalla stringa che viene restituita in output

7.2 Validazione

Garantisce che la copia eseguita è identica al dato originale.

7.3 Preservazione

Garantisce che non vengano eseguite `modifiche/alterazioni` alla copia, in caso contrario il valore di hash sarà differente

7.4 File LOG

File descrittivo in cui sono presenti le informazioni sulla copia forense realizzata:

- Informazioni sullo strumento impiegato;

- Informazioni sul disco di origine;
- Informazioni dell'immagine forense;
- HASH.

8 Lezione del 31-03 - Raccolta e Validazione - Disk Image e Tool

8.1 Disk image (Fine anni 60)

Mondo aziendale → disaster recovery

Mondo user → duplicazione supporti ottici (backup, facilitare la masterizzazione, diffusione `SW/utility`)

Formato VDMK, VDI, VHD, DMG.

8.2 Formato `DD/RAW`

Formato semplice → container dello stream.

Problematiche:

- Non conserva metadati dell'evidence;
- Non conserva hash calcolati;
- Non esegue compressione;
- Non può contenere più di un `file/stream`.

8.3 Expert witness Disk Image Format (EWF)

Presenta:

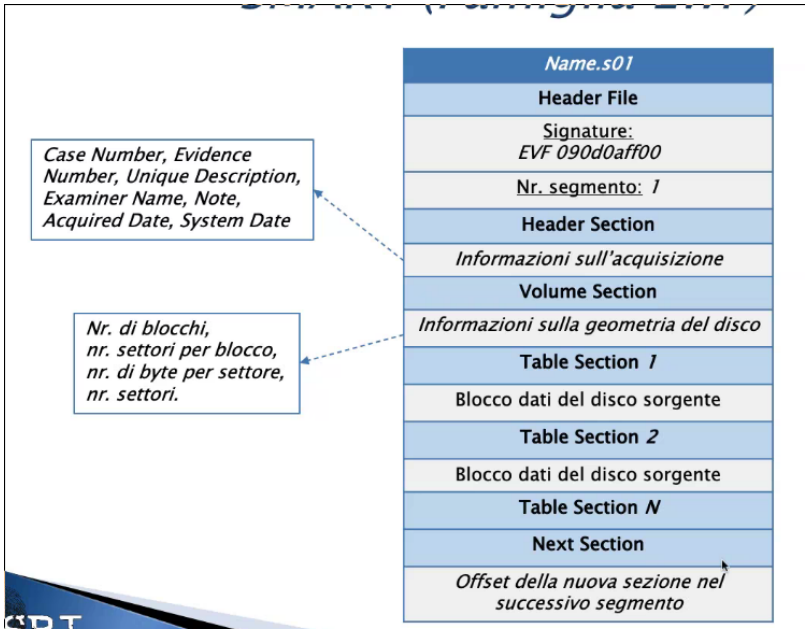
- File immagine composto in sezioni;
- compressione → algoritmo deflate;
- Segmentazione dell'immagine.

Lo scopo è quello di avere un accesso veloce ad una parte dell'immagine.

Ogni segmento presenta:

- Header file → *Signature e nr. di segmento*;
- Una o più sezioni
    1. *header section*;

2. *volume section*;
3. *table section*;
4. `next/done` *section*.



8.4 Encase E01 Bitstream

- Basato sul formato SMART;
- Segmentazione dell'immagine;
- Tre livelli di compressione
  - *no*;
  - *good*;
  - *best*.
- Impiega nr. 13 sezioni (+9 al formato SMART).

8.5 Encase LO1 Logicale (famiglia EWF)

- Acquisizione di file logici;
- Segmentazione dell'immagine;
- Impiega nr. 15 sezioni (+2 al formato E01).

8.6 Advanced Forensics Format (`AFF/AFF4`)

- Formato open ed estensibile;

- Creato prima dell'implementazione open source di libewf (2006);
- Ogni disco viene separato in 2 layer
  - disk-rapresentation layer (metadato);
  - data-storage layer (dato).

8.7 Tool di acquisizione

8.7.1 Guymanager

- Sviluppo da Guy Voncker;
- Licenza → Free OpenSource;
- Piattaforma → Linux;
- Basato sulla libreria libewf (clone + disk image);

Permette la full disk image soltanto

8.7.2 FTK Imager

- Prodotto dalla AcceData;
- Licenza → Freeware;
- Piattaforma → win (*lite* e *install version*)

9 Lezione del 12-04 - Protocolli Crittografati (Funzioni di Hash)

9.1 Crittografia

Crittografia → rendere oscuro ciò che scrivi o vuoi comunicare (letteralmente scrittura nascosta).

9.2 Crittologia

Disciplina che si occupa delle scritture nascoste.

9.3 Crittografia (Storia antica)

- Atbash → alfabeto rovesciato:
- Albam → alfabeto diviso in 2 metà;
- Atbah → relazione numerica fra le lette.

Tra i casi più famosi ricordiamo la lettera di Cesare a Cicerone.

9.4 Crittografia (Storia moderna)

Utilizzo dei PC e introduzione fondamenti matematici.

9.5 I protocolli

Un protocollo o schema definisce le interazioni fra le parti per ottenere le proprietà di sicurezza desiderate:

- Parti → entità coinvolte nello schema;
- Proprietò di sicurezza → privatezza etc.

I protoccoli si basano su una serie di protocolli più semplici detti **primitive crittografiche**:

- Risolvono problemi semplici;
- Posssono essere utilizzate per risolvere problemi più complessi.

Sono date da:

- Fonti (*es* DES);
- Problemi matematici (*es* teoria dei numeri).

9.6 Primitive

Risolvono i seguenti problemi:

- Cifratura → cifrari simmetrici e asimmetrici o a chiave pubblica;
- Autenticazione ed integrità → Funzioni HASH e MAC;
- Firme digitali;
- Altro → generazione di numeri pseudo-casuali, prove zero-knowledge.

9.6.1 Cifrario simmetrico

Condivisione della stessa chiave tra i 2 partecipanti A e B

9.6.2 Cifrario asimmetrico

Si impiegano 2 chiavi differenti:

- Chiave pubblica → impiegata per cifrare;
- Chiave privata → impiegata per decifrare;

9.6.3 Firma digitale

Apposizione di una firma ad un documento digitale. Proprietà:

- La firma digitale deve poter essere facilmente prodotta dal leggittimo firmatario;
- Nessun utente deve poter riprodurre la firma di altri;
- Chiunque può facilmente verificare la firma.

Algoritmi:

- RSA;
- Digital Signature Standard (DSS);

9.6.4 Primitive di HASH

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

Tra i suoi impiegi ricordiamo:

- Firma digitale;
- Integrità dei dati;
- Certificazione del tempo.

Integrità dei dati

Computo al tempo T_0 il valore hash del file M $\rightarrow$ $H = h(M)$.

Per controllare se il file è successivamente modificato ricalco il suo valore hash e lo confronto con quello precedentemente ottenuto.

9.6.5 Primitive MAC

Il loro impiego è:

- Integrità dei dati;
- Autenticità dei dati $\rightarrow$ verificare chi è stato il mittente dei dati.

9.6.6 Proprietà di sicurezza

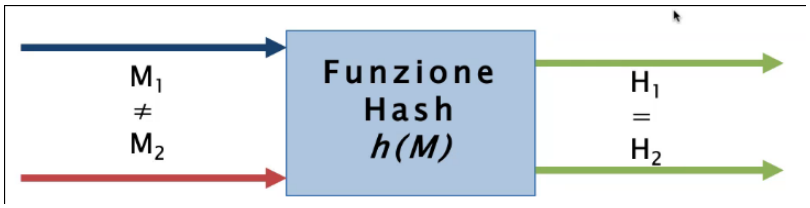
- Confidenzialità → protezione del dato da un soggetto estraneo;
- Autenticazione → certezza di identificare l'interlocutore;
- Integrità → verificare che il messaggio non sia stato modificato durante la trasmissione;
- Non-Ripudio → negare il disconoscimento del messaggio al mittente o destinatario;
- Anonimia → nascondere l'indentità di chi ha compiuto una determinata azione nel contesto crittografico.

9.7 Funzioni di Hash

9.7.1 Collisione

$$h: \sum * \rightarrow \sum^{n}$$

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



Esistono infinite collisioni

9.7.2 Proprietà

- One-Way → dato un hash y è computazionalmente difficile trovare M: $y=h(M)$;
- Sicurezza debole (2nd pre-image) → dato M è computazionalmente difficile trovare una variazione di M, M^1 tale che:

$$h(M) = h(M^1)$$

- Sicurezza forte (collision resistance) → computazionalmente difficile trovare 2 diversi messaggi con lo stesso valore hash.

Una One-Way Hash Function:

- Verifica le proprietà pre-image e 2nd pre-image resistant;

- Viene detta weak one-way has function.

Una Collision Resistant Hash Function:

- Verifica la proprietà di collision resistance;
- Viene detta strong one-way has function.

Una funzione f è One-Way se:

- Per ogni x nel dominio di f è facile calcolare $y=f(x)$, ma dato y, è computazionalmente inammissibile trovare x tale che $y=f(x)$.

Differenze con OWHF:

- Non ci sono limitazioni sul codominio;
- Non è richiesta la sicurezza debole

9.7.3 Costruzione della funzione

- Il messaggio input M viene diviso in k blocchi di lunghezza fissa $m_1, m_2, \ldots, m_k$;
- I blocchi vengono trattati in modo
  - `Seriale/Iterato` → una collisione per $h(M)$ implica una collisione di f (padding);
  - Parallelo → resistentee alle collisioni se lo è la funzione h.

Modello HASH a cascata

$$\mathrm{h(M)} = \texttt{H1(M) * H2(M)}$$

È dato dal prodotto di 2 funzioni hash → una collisione per h(M) vuol dire trovare una collisione sia per H1 che per H2

9.7.4 Cifrari a blocchi

- Cifrario a blocchi $\mathrm{E_k}$ per input ad n bit;
- Funzione g che da n bit produce una chiave;

10 Lezione del 14-04 - Protocolli Crittografati (Funzioni di Hash pt2)

10.1 `MD4/MD5`

- MD4 → progettata nel 1990 da Ron Rivest;
- MD5 → progettata nel 1991.
- Operazione efficienti su architetture 32 bit little-endian.

10.1.1 Little-endian e Big-endian

- Little-endian → il byte con indirizzo più basso è quello meno significativo;
- Big-endian → il byte con indirizzo più basso è quello più significativo;

10.1.2 Obiettivi

- Sicurezza forte;
- Sicurezza diretta;
- Velocità;
- Semplicità e Compatezza.

10.1.3 Padding del messaggio

`MD4/MD5` processa il messaggio in blocchi di 512 bit. Ogni blocco consta di 16 parole di 32bit.

M^1 sarà costituito da:

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

$$M^1 = M\ 100\ldots0\ (\rightarrow p)\ b$$

$$p \mid (p+M) \bmod_{512} = 448 \leftrightarrow 512 - [(M+b) \bmod_{512}]$$

M^1 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 = $\frac{N}{16}$ di 512 bit

10.1.4 Operazioni

Impiegano diverse operazioni sulle word in input X e Y restituendo una nuova word:

- $(X \wedge Y) \rightarrow$ and bit a bit di X e Y;
- $(X \vee Y) \rightarrow$ or bit a bit di X e Y;
- $(X \oplus Y) \rightarrow$ xor bit a bit di X e Y;
- $(\neq X) \rightarrow$ complemento bit a bit di X;
- $(X + Y) \rightarrow$ somma intera modulo 2^{32};
- $(X \ll s) \rightarrow$ shit circolare a sinistra di s bit;

10.1.5 Round

1. $F(X,Y,Z) = (X \wedge Y) \vee ((\neq X) \wedge Z)$;
2. $G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge (\neq Z))$;
3. $G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge Z) \vee (X \wedge Y)$;
4. $H(X,Y,Z) = X \oplus Y \oplus Z$;
5. $I(X,Y,Z) = Y \oplus (X \vee (\neq Z))$.

X	Y	Z	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

10.1.6 Funzione di compressione

3 round per MD4 e 4 per MD5. Ogni round prende in input:

- Blocco corrente di 512 bit = 16 wor;
- Valore corrente del buffer, 4 word ABCD per 128 bit;
- Ogni round consiste in 16 operazioni;
- L'output dell'ultima fase viene sommato all'input della prima fase
  - la somma avviene word a word;

- L'output della L-esima fase è il digest a 128 bit.

Funzione di compressione per MD4

Ogni round consiste di 16 operazioni, ognuna delle quali agisve sul buffer di 4 word A.B.C.D

$$t = (A + W(B,C,D) + X[j] + Y[J]) \ll s[j]$$

$$(A,B,C,D) = (D,T,B,C)$$

Dove:

- X[j] $\rightarrow$ è predefinito e reperibile all'interno dell'algoritmo;
- s[j] $\rightarrow$ indica lo shift ciclico;
- y[j] $\rightarrow$ costante additiva relativa al round corrente;
- W $\rightarrow$ funzione del round (F,G,H).

Funzione di compressione per MD5

Ogni round consiste di 16 operazioni, ognuna delle quali agisve sul buffer di 4 word A.B.C.D

$$A \leftarrow B + ((A + W(B,C,D) + X[k] + T[i])) \ll s$$

Dove:

- K $\rightarrow$ indice della parola;
- s $\rightarrow$ indica lo shift ciclico;
- i $\rightarrow$ indice dell'interazione;
- W $\rightarrow$ funzione del round (F,G,H,I);
- X[k] $\leftarrow M^1[16i + k]$ è la k-esima word di 32 bit nell'i-esimo blocco;
- T[i] $\rightarrow$ i-esimo elemento della tabella di 64 valori.

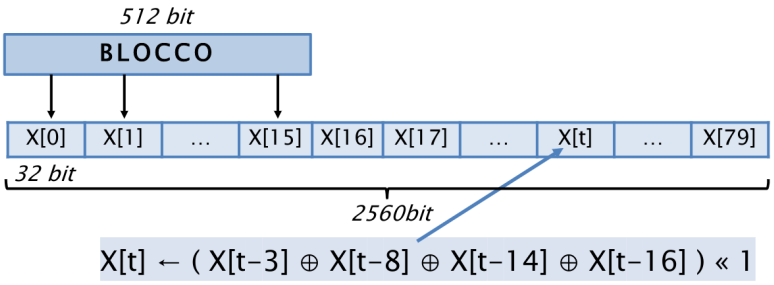
10.1.7 Differenze

MD5	MD4
4 round (4x16 operazioni)	3 round (3x16 operazioni)
4 funzioni logiche	3 funzioni logiche
64 costanti additive	2 costanti additive
Ogni passo aggiunge il risultato del passo precedente	

10.2 SHS/SHA

- Secure Hash Standard;
- Secure Hash Algorithm;
- Standard del Governo USA dal 1993;
- Operazioni efficienti su architettura 32 bit big-endian;
- Stessi principi di MD4/MD5, ma più sicuro;
- Presenta un padding pressochè identico alla famiglia MD.

10.2.1 Espansione blocco ed iterazioni



- 4 round di 20 operazioni ciascuna (80 iterazioni);
- Per ogni iterazione una parola X[i] viene calcolata dal blocco input

10.2.2 Funzioni

1. t = 0,...,19: F(t,X,Y,Z) = (X $\wedge$ Y) $\vee$ (($\neq$ X) $\wedge$ Z); (if X then Y else Z)
2. t = 20,...,39: F(t,X,Y,Z) = X $\oplus$ Y $\oplus$ Z; (bit di parità)
3. t = 40,...,59: F(t,X,Y,Z) = (X $\wedge$ Z) $\vee$ (Y $\wedge$ Z) $\vee$ (X $\wedge$ Y); (2 su 3)
4. t = 60,...,69: F(t,X,Y,Z) = Y $\oplus$ X $\oplus$ Z; (bit di parità)

X	Y	Z	F(0,...)	F(20,...)	F(40,...)	F(60,...)
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

10.2.3 Differenze

- Sicurezza forte → maggiore in SHA-1;
- Sicurezza contro l'analisi → MD5 soggetta ad alcuni attacchi;
- Velocità → entrambi con algoritmi molto veloci;
- Semplicità e compattezza → semplice da descrivere e da implementare, nessun uso di tabelle e di complesse strutture dati.

11 Lezione del 21-04 - L'analisi (Gli strumenti pt.1)

11.1 L'analisi

Per una corretta analisi di un dato vanno rispettati i seguenti punti:

- Va eseguita su una copia;
- Deve essere riproducibile;
- Bisogna ottenere lo stesso risultato da diverse `operazioni/strumenti` di analisi;
- Ricostruzione di eventi passati mediante la lettura di dati digitali.

Il primo strumento di analisi è il proprio bagaglio di conoscenze informatiche

11.2 Montare un file immagine

Si analizza il disco con una utility (es fdisk) con cui andremo a listarne il contenuto e andremo in seguito a montarlo con il comando mount e una serie di flag:

$$\text{mount -o ro,loop,offset= } \textit{offset} \text{ =disco posizione}_{\text{dovemontarlo}}$$

Dove:

- ro → read-only;
- loop → crea un virtual block device da un file;
- offset=byte → punto di inizio della partizione da montare

È possibile poi fare il **merge** attraverso il comando *affuse* o con il comando *ewfmount* (caso immagine segmentata EWF)

affuse `/mnt/dest/dd_image/sda.000 /mnt/sda_fuse`

ewfmount `/mnt/dest/dd_image/sda.E01 /mnt/sda_fuse`

11.2.1 Pro e contro

Pro	Contro
Veloce per operazioni semplici	Farraginoso
Utilizzo di tool non forensic oriented	Solo file residenti
	Riconoscimento del FileSystem dell'immagine demandata al nostro SO

11.3 Strumenti SW

11.3.1 Toolkit

Supporto all'intera fase di analisi.

11.3.2 Tools Forensic Oriented

Esecuzione di uno specifico task.

11.3.3 Tool Generici

Non progettati per la CF.

12 Lezione del 26-04 - L'analisi (Gli strumenti pt.2)

12.1 I Toolkit (Formati File Immagine)

- Forensic ToolKit (FTK) → commerciale (su macchine win)
  - Encase E01;

  - Encase L01 logical;
  - Expert Witness;
  - SnapBack 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 → Free e OpenSource (multipiattaforma)

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

12.1.1 File System supportati

FTK	Autopsy
FAT	FAT
exFAT	exFAT
NTFS	NTFS
Ext2FS	Ext2FS
Ext3FS	Ext3FS
Ext4FS	Ext4FS
APFS	APFS
HFS	HFS
HFS+	HFS+
CDFS	YAFFS2
ReiserFS 3	
VxFS (Veritas FS)	

12.1.2 Le viste

Offrono più visualizzazioni delle informazioni contenute nella copia forense → elaborazione di file e artefatti.

Vista ad albero → tipo di rappresentazione gerarchica dei file.

12.1.3 Catalogazione

Analisi dei file per:

- Estensione (suffisso del file);
- Signature (magi number) → sequenza di bit posta in punt ben preciso del file (offset), normalmente prima della sequenza di dati, che serve per definire il formato in cui i dati sono memorizzati.

12.1.4 Classificazione

I file vengono analizzati ed arricchiti di alcuni attributi:

- Bad extension → *estensione* vs *signature*;
- Delete file → file marcati come cancellati dal file system.

12.1.5 Known file

Riconoscimento del file basato sull'hash.

Ignorable File

File conosciuti come di non interesse:

- Sottrazione di migliaia di File dall'analisi.

Notable File

File conosciuti come di notevole interesse:

- Ricerca mirata di determinati file.

12.1.6 Artefatti

Analisi del contenuto del file:

- Estrazione ed elaborazione delle informazioni presenti in uno o più file.

Metadati

Dati strutturati contenenti informazioni aggiuntive sul file.

e-Mail Archive

Analisi degli `archivi/database e-Mail`:

- Visualizzazione delle `E-mail`;
- Estrazione degli allegati.

System Information

Estrazione delle informazioni dell'ambiente di lavoro

User Activity

Analisi delle attività eseguite dall'utente.

Navigazione Web

Analisi dei file dei browser web.

Image Gallery

Generazione e visualizzazione di *thumbnail* dei file grafici.

Video Gallery

Processo di elaborazione per l'estrazione e la visualizzazione di frame dai video

Social Analyzer

Visualizzazione delle `relazioni/connessioni` avvenute tra i diversi soggetti.

TimeLine

Visualizzazione temporale dei file.

12.1.7 Altri strumenti

File Carving

Recupero dei file non più residenti nel file system.

Ricerca semi manuali

- Ricerva tramite attributi;
- Document Content → estrazone di determinate informazioni mediante regular expression;
- Indexing → ricerca di determiante parole chiave.

Citiamo inoltre:

- Decrypt;
- Malware Analysis;
- Processing Image
  - PhotoDNA;
  - Riconoscimento `Immagine/Viso`;
  - Traduttore.

12.1.8 `Export/Report`

Esportare i file di interesse:

- `Etichette/Tag`;
- Checkbox.

13 Lezione del 28-04 - Autopsy

Programma che presenta 2 modalità:

- Single user;
- Multi user.

13.1 Configurazione - Central Repository

Database in cui vengono memorizzate le informazioni di casi precedentemente analizzati:

- Conoscere se un file è già stato rinvenuto;
- Evidenziato automaticamente un file come di notevole interesse (notable file);
- Case DB più leggero.

13.2 Ingest Modules

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

- Hashing;
- Identificazione del file type;
- User Activity
  - Analisi dei registri;
  - Analisi del browser;
- Indexing
- File Carving

13.3 Ingest Manager

Esegue i processi di analisi in background → file vengono processati in base alla seguente priorità:

- Cartelle utenti;
- Program Files e altre cartelle nella root;
- Cartella di Windows;
- Spazio non allocato

È presente una esecuzione parallela di più file immagini. I risultati sono visualizzabili nella sezione "result"

13.3.1 Hash Lookup

Calcola l'hash MD5 per ogni file. Memorizza gli hash nel Case DB. Ricerca gli hash calcolati all'interno di una lista di *Known Hash*:

- Known as Ignorable file (NSLR);
- Known as Notable File.

Ogni file nel caso ha 3 valori di *Known Status*:

- Unknown (default);
- Known (ignorable);
- Notable (Known bad).

Nel caso di Known files avremo 3 possibilità:

- Possono essere ignorati anche dagli altri moduli;
- Possono essere nascosti dalla "views" area (default);
- Possono essere nascosti dalla vista ad albero (not default).

Questo velocizza notevolmente l'analisi

13.3.2 File Type

Determina la tipologia del file analizzando la signature. Questo viene poi conservato nel Case DB → molti moduli dipendono da queste informazioni.

È basato sulla libreria Tika:

- Viene impiegato la cataloazione MIME type.

13.3.3 File Extension Mismatch

Per ciascun file confronta l'estensione con la propria categoria → se le informazioni non sono coerenti viene etichettato.

Questo dipende dal modulo "File Type". L'obiettivo è trovare file che l'utente abbia provato a nascondere.

13.3.4 Embedded File Extractor

Estrae i file incapsulati in altri file:

- Archive File (Zip, Rar,...);
- File grafici da Documenti `Office/PDF`.

I file estratti vengono salvati nel Case Folder → risultati sono visionabili nella "tree view". Vengono etichettati se protetti da password.

13.3.5 Email parser

Ricerca ed analizza archivi di posta:

- Mbox;
- PST;
- EML file.

I risultati sono visualizzabili nella sezione "result" nella categoria "E-Mail Messages":

- Gli allegati sono trattati come figli del messaggio;
- Sono raggruppati in *threads*.

È possibile analizzarli dettagliatamente attraverso la vista "Comunications".

13.3.6 Interesting Files

Etichetta file e cartelle che si pensa essere *interessanti*:

- Viene notificato il rinvenimento di tali oggetti.

13.3.7 Encryption Detection

Etichetta file e volumi che `sono/potrebbero` essere cifrati:

- Documenti `Office/PDF` e Acces DB protetti da password;
- Possibili file o volumi con cifratura basato su
  - High Entropy;
  - Dimensione multiplo di 512 byte;
  - Tipo di file sconosciuto.

13.3.8 Plaso

Tool open che esegue il *parsing* di file log e altri tipi di file per esttrarre i **timestamp**:

- Estrae quanti più timestamp possibili per l'elaborazione di una timeline;
- Operazione molto lunga.

13.3.9 Virtual Machine Extractor

Analizza le VM presenti all'interno del reperto:

- Ricervaa i file VMDK e VHD;
- Crea una copia locale;
- Vengono inseriti in *datasources*.

13.3.10 Data Source integrity

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

Recupera l'hash dai metadati del disk image oppure da quelli inseriti dal CF.

Calcola l'hash del disk image. Invia un alert se la validazione fallisce.

14 Lezione del 03-05 - Autopsy pt2

14.1 Ingest Modules - Recent Activity

Estrae le attivivtà recenti dell'utente:

- Analisi del web browser;
- Analisi dei registri;
  - Dispositivi USB;
  - Lista utenti;
  - Programmi installati;
  - Programmi eseguiti;
- Analisi del *cestino*.

I risultati vengono poi inseriti in *Extracted Content*

14.1.1 Analisi registri

Analisi delle chiavi di registro mediante RegRipper:

- Tool OpenSource
- Analizza il contneuto 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.

14.1.2 Recycle Bin

Analisi del file cancellati ed ancora presenti nel "cestino".

Cambio del filename:

- $\geq$ Windows 7 $\rightarrow$ $=R + [randomnumbers/letter]$
- < Windows 7 $\rightarrow$ `D+[drive letter] + [random numbers/letters]`
- 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*

Risultati:

- Artefatto *Recycle Bin*;
- Creazione di un *delete file* nella vista ad albero (*data sources*);

14.1.3 Keyword Search

`Genera/Aggiorna` un text index $\rightarrow$ Abilita la ricerca testuale.

1. Si estrae ogni wrod da ogni file;
2. Se la word non esiste viene aggiunta;
3. Associa la word all'ID del file.

Uso di **Apache Solr**:

- Indice memorizzato all'interno del *case folder*.
- Contiene:
  - File name;
  - Testo estratto dal contenuto del file;
  - Testo estratto dagli artefatti.

Uso di **Apache Tika** per l'estrazione del contenuto dei file e dei metadati:

- Per file non riconosciuti o corrotti → **string extractor** (ricerca per byte (encoding, languages)).

Uso di un proprio *HTML Text Extractor*. Estrazione anche di *commenti* e *java script*.

Nromalizzazione:

- Ricerche case insensitive;
- Unicode.

14.1.4 Correlation Engine

Ricerca dei file del caso all'interno di un *Central Repository*:

- Correlare il Caso corrente con i Casi passati:
  - Evidenzia il `file/item` che erano stati etichettati come *Notable* nei casi precedenti.

Aggiorna il *Central Repository* con i file del caso corrente:

- Consente di correlare nuovi Casi al caso corrente

Il *Central Repository* conserva:

- Valore (Hash, Phone Numbers, Email address...);
- Caso;
- Data Source;
- File Path;
- Commento del CF;
- Notable Status.

14.1.5 PhotoRec Carver

Recupero dei file cancellati mediante *PhotoRec*:

- Tool OpenSource;
- Data Carving;
- Lavora su *unallocated space*.

Risultati → nella vista ad albero `$CarvedFile`.

14.1.6 Android Analyzer

Analizza i dispositivi Android:

- Database di Android e app di terze parti;
- Acquisiszione fatta mediante altri strumenti.

Estrae:

- Registro chiamate;
- Contatti;
- Messaggistica;
- Browser;
- Geolocalizzazione.

14.2 Viste specializzate

14.2.1 TimeLine Graphic Interface

Consente di visualizzare graficamente le attività del sistema ordinate temporalmente:

- File Time estratti dal *File System*;
- Web Activity estratti dal *Recent Activity*;
- Exif;
- Plaso;
- . . . ;

14.2.2 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:

- Priorità
  - Numero di risultati positivi sull'hash;
  - Numero di `immagini/video`.

14.2.3 Comunication Interface

Visualizza i dati delle comunicazioni in modo differente:

- E-Mail Parser;
- Android Analyzer.

È orientato intorno agli account:

- Vengono visualizzate tutte le attività associate;
- Vengono visualizzate le relazioni con gli altri account.

14.2.4 Golocation

Riepiloga tutti gli artefatti in cui sono stati estratte le informazioni sulle posizioni:

- Exif Parser.

14.3 Tag & Report

14.3.1 Tagging

Creare un riferimento ad un `file/item` di interesse:

- Consente di commentarlo;

- Consente di etichettare solo una parte di una immagine,

Sono associati all'esaminatore:

- Conoscere chi li ha etichettati;
- Possono essere nascoste le etichette degli altri esaminatori.

Obiettivo:

- Ritrovare facilmente il file di interesse;
- Evidenziarlo ed esportarlo nel Report.

14.3.2 Comments

Consente di annotare il motivo dell'interesse di un `file/item`:

- Verrà visualizzato nel Report;
- Può essere salvato nel *Central Repository*.

14.3.3 Reporting

Generare un report per:

- Esportare e condividere i risultati dell'analisi;
- Unirlo ad altri report.

Salvato nella sezione *Reports*:

- Può essere elaborato da ulteriori *ingest modules*.

14.3.4 Portable Case

Versione più piccola del Caso originale:

- Solo i file etichettati;
- Solo i file presenti nella categoria *Interesting Item*.

Presenta un proprio DB SQLite. I file vengono esportati nel CaseFolder.

14.4 Extensible

Autopsy è costituito da moduli *plug-in*:

- DataSource Processor;
- Ingest Module;
- Content Viewer;
- Machine Translation;
- Report Module.

Gli utenti possono creare e pubblicare dei proprio plug-in (attraverso il repository di autopsy).

Linguaggio:

- Java;
- Python.

14.4.1 Java Module

Sono file con estensione `.nbm`:

- Possono contenere più moduli;
- L'IDE Netbeans consente di auto-aggiornarli e scaricarli.

14.4.2 Python Module

Sono cartelle che contengono file con estensione `.py`:

- Copia manuale delle cartelle in una specifica directory;
- Possono essere solo *Ingest Module* e *Report Module*.

15 Lezione del 10-05 - L'analisi : I Volumi

15.1 Volume System

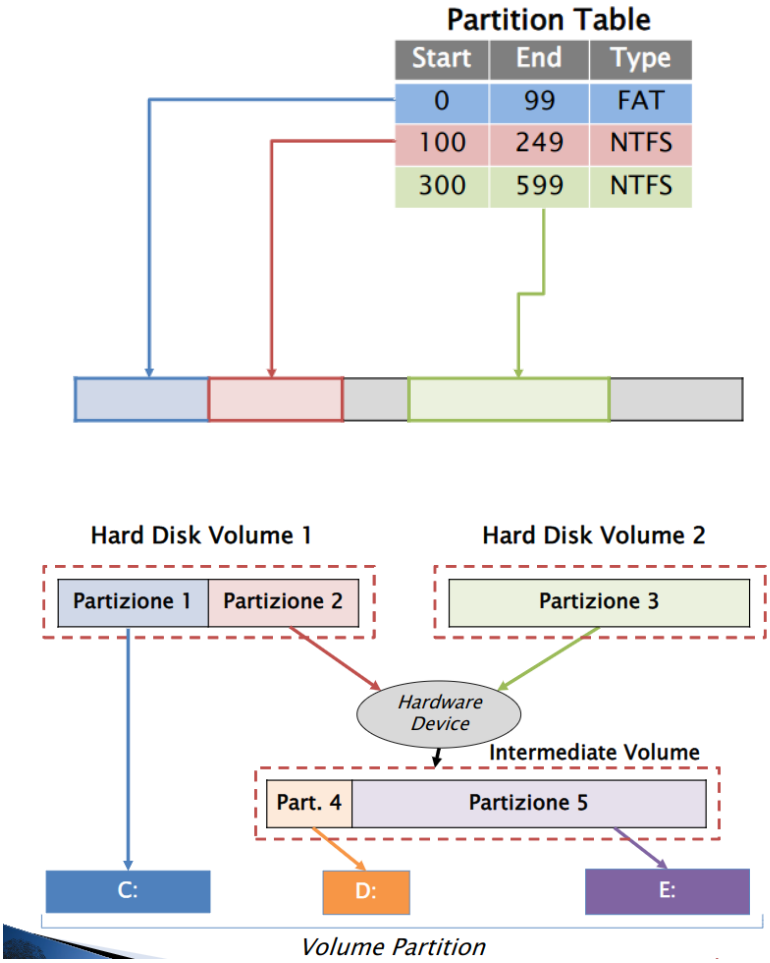
Si preoccupa di gesire i volumi per raggiungere 2 obiettivi:

- Unione di più volumi in un unico grande volume;
- Suddivisione del volume in partizioni.

Volume → insieme di settori per memorizzare dati.

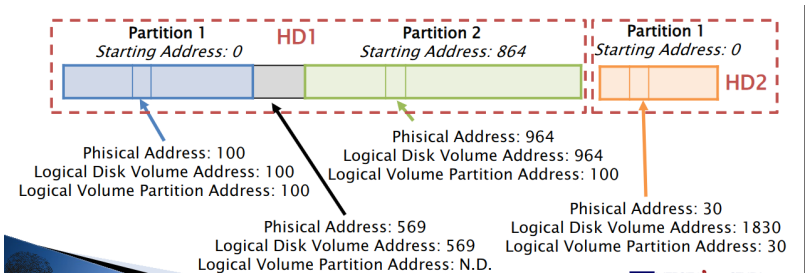
Partizione → insieme di settori consecutivi in un volume.

15.2 Partition Table



15.3 Indirizzamento dei settori

- LBA (Phisical Address) → 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.

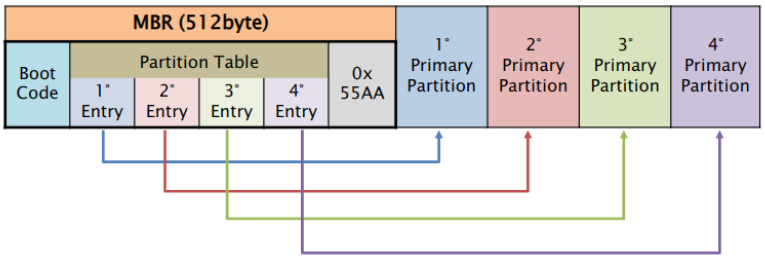


15.4 DOS Partition

Sistema di partizione più comune.

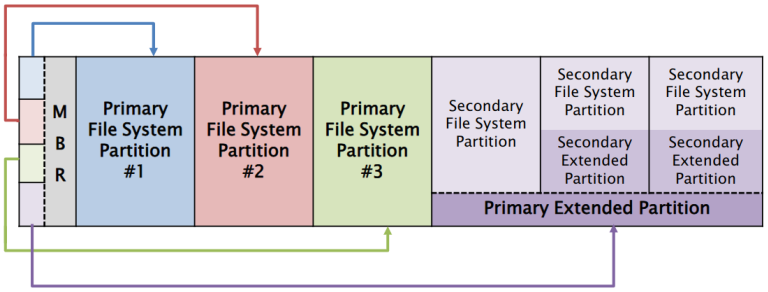
MBR (Master Boot Record) → presenta obbligatoriamente un primo settore di 512 byte:

- Boot Code;
- Partition Table (max 4)
  - Starting CHS address;
  - Ending CHS address;
  - Starting LBA address;
  - Numbers of sector in partition;
  - Type of partition;
  - Flags;
- Signature → `0x55AA`



- **Primary File System Partition** → partizione primaria che contiene un file system
- **Primary Extended Partition** → partizione primaria che contiene altre partizioni;
  - Tabella di partizione;
  - **Secondary File System Partition** → partizione secondaria che contiene un file system (partizione logica);
  - **Secondary Extended Partition**

* Tabella di partizione;
* Secondary File System Partition;
* Secondary Extended Partition
  - ...



15.4.1 Boot Code

Situato nei primi 466 byte del primo settore (MBR):

- Microsoft Boot Code → processa la tabella di partizione e ricerca ed identifica quella `c.d.` *bootable*, tramite FLAG;
- Possibile incapsulamento di virus;

Il settore MBR viene allocato all'inizio del *Disk Volume* e di ogni *Extended Partition*:

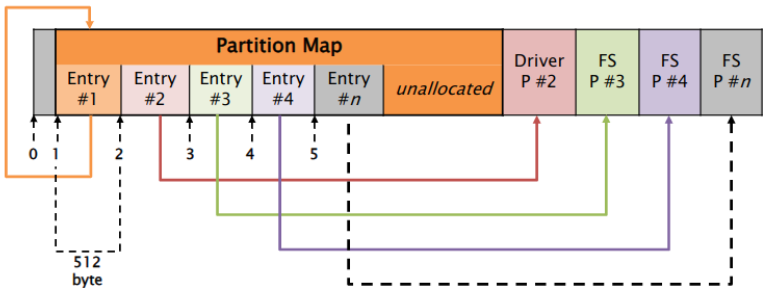
- EBR (Extended Boot Record) (512 byte)
  - La parte riservata al *Boot Code* è inutilizzata;
  - La parte riservata alle altre 2 entry nella *Partition Table* è vuota.

15.5 Apple Partition Map (APM)

- Impiegato soprattutto dai vecchi sistemi basati su processori non Intel;
- Nessun limite massimo di partizioni;
- Gestisce volumi fino a 2TB.

Partition Map → secondo settore (512 byte):

- Ogni entry (512 byte) descrive una partizione;
- La prima entry descrive la *Partition Map*.



Byte Range	Description	Essential
0-1	Signature value (0x504D)	No
2-3	Reserved	No
4-7	Total number of partition	Yes
8-11	Starting sector of partition	Yes
12-15	Size of partition in sectors	Yes
16-47	Name of partition in ASCII	No
48-79	Type of partition in ASCII	No
80-83	Starting sector of data area in partition	No
84-87	Size of data aerea in sectors	No
88-91	Status of partition	No
92-95	Starting sector of boot code	No
96-99	Size of botto code in sectors	No
100-103	Address of boot loader code	No
104-107	Reserved	No
108-111	Boot code entry point	No
112-115	Reserved	No
116-119	Boot code checksum	No
120-135	Processor type	No
136-511	Reserved	No

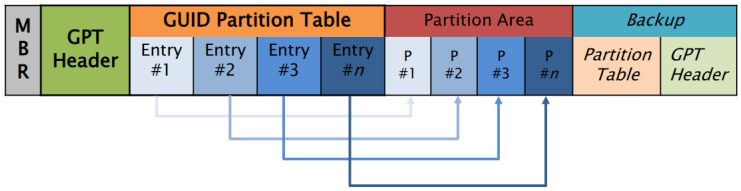
15.6 Guid Partition Table (GPT)

Sistema di partizionamento utilizzato da EFI:

- Massimo 128 partizioni;
- Volumi più grandi di 2TB.

Composto da 5 `aree/sezioni`:

- Protective MBR → DOS partition Table (1° settore);
- GPT Header → definisce il layout delle aeree;
- Partition Table → Ogni entry descrive la partizione;
- Partition Area → locazione riservata alle partizioni;
- Backup Area → copia di backup del GPT Header e della partition Table.

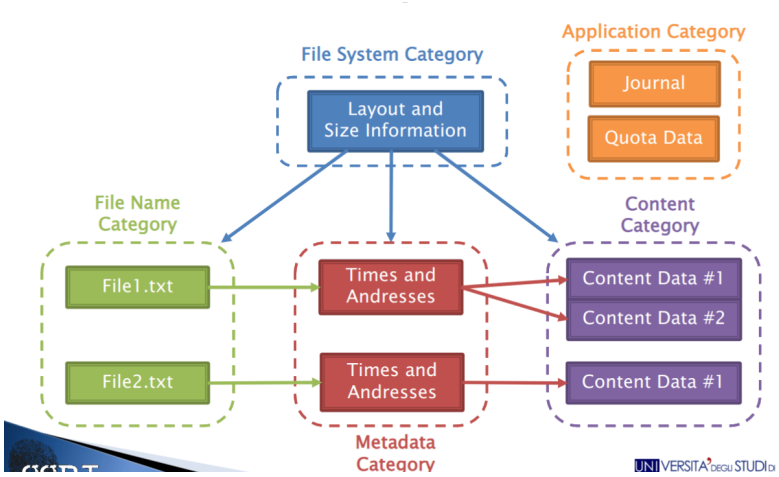


16 Lezione del 12-05 - L'analisi : I File System

16.1 Overview

Lo scopo di una analisi di un file system è quello di analizzare il contenuto dei dati contenuti in un volume.

Un file system è un sistema che permette la memorizzazione dei dati, organizzandoli gerarchicamente in file e directory.



Dati Essenziali	Dati Non Essenziali
Dati che se modificati `modificati/alterati` causano il malfunzionamento del sistema	Informazioni accessorie

Sono Dati essenziali (trusted data):

- Indirizzamento del contenuto del file;
- Nome del file;
- Dimensione del file.

Sono Dati non essenziali (untrusted data):

- Dati temporali;
- Permessi utente.

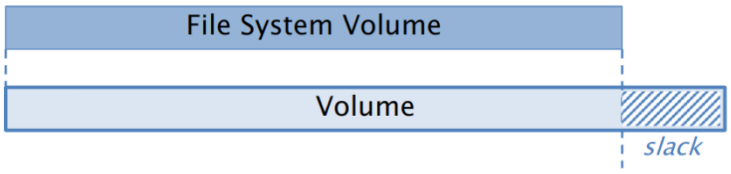
16.2 File System Category

Informazioni generali sul file system:

- Solitamente posizionati nel primo settore;
- Essenziali → informazioni sul layout dei dati.

Analisi:

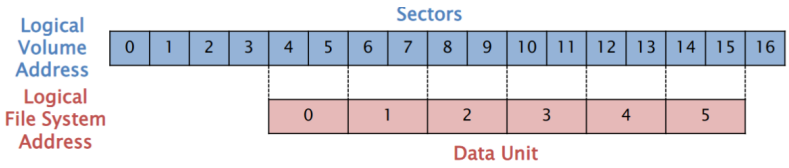
- Informazioni sulla generazione del file system;
- Informazioni sul layout;
- Controllo di consistenza → *volume slack*.



16.3 Content Category

Locazioni di memoria impiegate per la memorizzazione del contenuto dei file:

- Data Unit → raggruppamento di più settori
  - STATO → allocato o non;
  - Logical File System address



16.3.1 Strategia del primo disponibile

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

16.3.2 Strategia del prossimo disponibile

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

16.3.3 Strategia del più adatto

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

16.4 Content Category - Analisi

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

16.5 Metadata Category

Descrivono i file presenti in *content category*:

- Informazioni temporali → data di `creazione/accesso/modifca`;
- Indirizzo delle Data Unit allocate per il file.

Analisi:

- Ricerca di maggiori informazioni su di un file;
- Ricerca di file in base agli attributi descritti in questa categoria (*es.* file creati dopo una certa data).

16.5.1 Logical File Address

Indirizzo di parte del file allocata nella data Unit:

- È contenuto nella data unit.

16.5.2 Slack Space

Parte non usata di una Data Unit allocata.

16.5.3 File Recovery

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

16.5.4 Compressed File

Memorizzare i dati in un formato compresso occupano meno Data Unit.

3 livelli di compressione:

- Compressione dei soli dati all'interno del file
  - *es.* JPEG, mp3, . . . ;
- Compressione di tutto il file → creazione di un nuovo file.
- Compressione eseguita dal File System → invisibile lato applicativo e utente.

16.6 File name Category

Nome assegnato a ciascun file :

- nome del file → indirizzo della struttura metadato.

File Recovery:

- Recupero dei file cancellati ricercando i *File Name* con lo stato non allocato
  - Analisi della struttura metadati indirizzata

16.7 Application Category

Dati non essenziali al file system:

- Sono più efficaci se conservati nel File System (*es* Spazio occupato, Journaling).

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

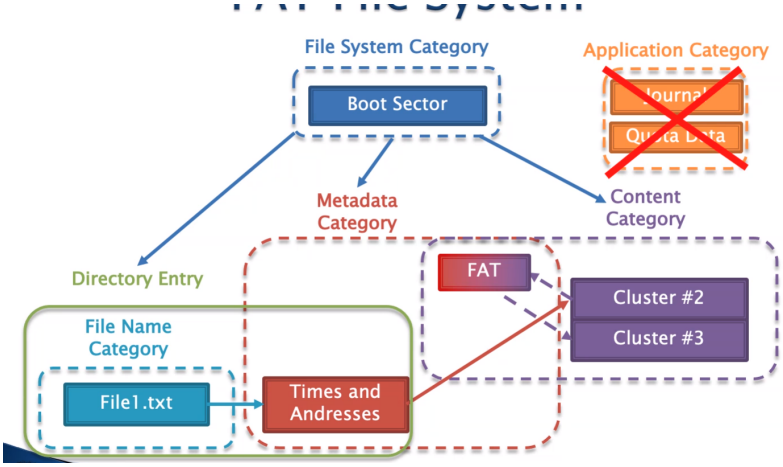
- Evitare l'inconsistenza

- Completamento delle operazioni di modifica;
- Rollback.

Analisi → ricostruire eventi di un incidente recente.

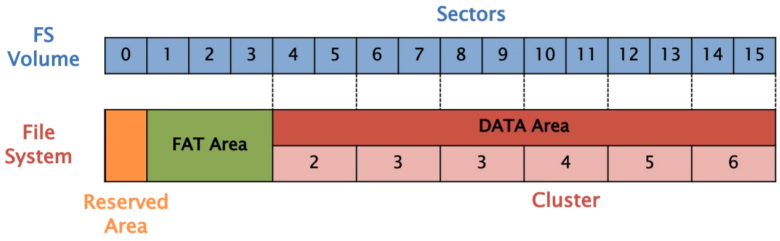
17 Lezione del 17-05 - L'analisi : I File System (pt2)

17.1 FAT File System (File Allocation Table)



Contiene dati che rientrano sia nella Content Category sia nella Metadata Category

17.2 Physical Layout



17.3 FAT - File System Category

- FSINFO (FAT32) → Reserved Area (BootSector)
  - Cluster liberi;
  - Prossimo cluster libero.
- Boot Sector → primo settore (Reserved Area)
  - Physical Area → settore 0

    * FAT `12/16` → dimensione 1 settore;
    * FAT 32 → dimensione variabile
  - FAT Area → dopo la reseved area
    * Dimensione → `SIZE FAT x Nr.  FAT`;
  - Dat Aerea → successiva alla FAT Area
    * Dimensione → `tot settori - inizio Area`;
    * Dimensione cluster;
    * Root Directory (FAT 32);
      · Dimensione (`FAT 12/16`).

17.3.1 Boot Sector

Primo settore (Reserved Area)

- Non Essential Data
  - OEM Name → info strumento creazione del FS;
  - Volume Serial Number → data di creazione (Microsoft);
  - File System Label → `FAT, FAT12, FAT16, FAT32`.

Nel caso di FS `FAT 12/16`

Byte	Descriptor	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 32 kb]	SI
14-15	Dimensione Reserved Area (Settori)	SI
16	Nr. di FAT (solitamente 2)	SI
17-18	MAx nr. File in root directory [FAT `12/16`][0 FAT32]	SI
19-20	Tot Settori FS	SI
21	Media Type [dischi removibili o non]	NO
22-23	Dimensione FAT (settori) [FAT `12/16`][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	NO
36 37 38	BIOS INT. 13H Non usato Extended boot signature (identifica se i successivi 3 valori sono validi)	NO NO NO
39-42	Volume Serial Number	NO
43-53	Etichetta volume (ASCII)	NO
54-61	File System type	NO
62-509	Non Usato	NO
510-511	Signature	NO

Nel caso di FS `FAT32`

Byte	Descriptor	Es.
36-39	Dimensione della FAT	SI
40-41	Nr. di FAT	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	NO
52-63	Riservati	NO
64	BIOS INT.	NO
65	Non usato	NO
66	Extended boot signature (identifica se i successivi 3 valori sono validi)	NO
67-70	Volume SN	NO
71-81	Etichetta volume (ASCII)	NO
82-89	File System type	NO
90-509	Non usato	NO
510-511	Signature	NO

17.3.2 FSINFO

Byte	Descriptor	Es.
0-3	Signature	NO
4-483	Non usato	NO
484-487	Signature	NO
488-491	Nr. di cluster liberi	NO
492-495	Prossimo Cluster libero	NO
496-507	Non usato	NO
508-511	Signature	NO

17.4 Analisi

Recuperare informazioni sul layout

Controllare possibili dati nascosti:

- Bootcode;
- Settori in Reserved Area →
  - FSINFO;

- Volume slack;

Confronto tra il boot sector ed il backup del Boot Sector.

17.5 Content Category

- Contenuto di File e directory
- Cluster $\rightarrow 2^x$ settori (max `32KB`)
  - Primo Cluster $\rightarrow$ indirizzo 2;
  - Solo in Data Area.

17.6 FAT

Identificare lo stato di allocazione dei Cluster

Successivo cluster del file $\rightarrow$ **Cluster Chain**

Layout $\rightarrow$ Boot Sector

Entry di ugual dimensione:

- FAT12 $\rightarrow$ 12 bit;
- FAT16 $\rightarrow$ 16 bit;
- FAT32 $\rightarrow$ 32 bit.
- Entry = Cluster
  - Cluster non allocato $\rightarrow$ 0 ZERO;
  - Cluster allocato
    - Prossimo cluster
    - EOF
      - FAT12 $\rightarrow$ `0xff8`;
      - FAT16 $\rightarrow$ `0xfff8`;
      - FAT32 $\rightarrow$ `0xfff fff8`;
  - Cluster Danneggiato
    - FAT12 $\rightarrow$ `0xff7`;
    - FAT16 $\rightarrow$ `0xfff7`;
    - FAT32 $\rightarrow$ `0xfff fff7`;

17.6.1 Indirizzamento

La prima entry ha indirizzo 0 ZERO.

L'indirizzo entry è uguale all'indirizzo Cluster:

- Entry[0] → informazione del media;
- Entry[1] → dirty status.

17.7 Metadata Category

Informazioni su file e directory:

- Indirizzo del primo cluster;

Parent Directory:

- Directory Entry → `32KB`;
  - File
  - Directory.

Posizionata nella Data Area (Cluster)

File Name Category:

- Nome File (8 caratteri) + Estensione (3 caratteri);
- > Long File NAme Directory Entry

Byte	Descriptor	Es.
0	Primo carattere del filename	SI
1-10	Caratteri da 2 a 11 del filename	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)	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	SI

17.7.1 Attributi

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)	Archivio	NO

17.7.2 Informazioni Temporali (non essential data)

Data di creazione:

- Nuovo `File/Copia` → Nuova data;
- `Sposto/Rinomino` → copia della data.

Modifica del contenuto:

- `Copia/Sposto/Rinomino` File → copia della data.

Data di Accesso:

- Modificata anche visualizzando le proprietà

17.7.3 File Name Category

Mappare le strutture *Metadata* con un etichetta → Filename.

Directory Entry → insieme ai *metadata category*:

- FileName → 11 caratteri;
- Long File Name (LFN) directory entry → + 13 caratteri.

18 Lezione del 19-05 - L'analisi : I File System (pt3)

18.1 NTFS (New Technologies File System)

Ogni cosa è un file. File System scalabile

Gestisce tutto attraverso i file.

18.2 Master File Table (`$MFT`)

Contiene informazioni su file e directory:

- Ogni `file/directory` ha almeno 1 entry (File Record)
  - 1024 byte (boot sector)
- Entry[0] → `$MFT`
- Starter Cluster (Boot sector)

MFT Entry

Ha una dimensione di 1024 byte:

- Presenta un Header di 42 byte;
- Presenta attributi quali strutture dati;
- Presenta Signature del tipo `«FILE»/«BAAD»`;
- Presenta uno stato di allocazione → attributo `$BITMAP` nella entry[0] `$MFT`;

- Presenta un indirizzo sequenziale → 48 bit (File Number);
- Presenta un numero sequenziale → 16 bit (contatore allocazione).

Byte	Descriptor	Es.
0-3	Signature (ASCII) `[File/BAAD]`	NO
4-5	Offset to fixup array	YES
6-7	Number of entries in fixup arrat	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 referenc to base record	NO
40-41	Next Attribute ID	NO
42-1023	Attributes and fixup values	YES

18.3 File System Metadata

File contenenti dati per l'amministrazione del FS. Le prime 12 entry sono:

- `$MFT` → MFT Entry;
- `$MFTMirr` → MFT Backup;
- `$LogFile` → Journal;
- `$Volume` → Volume info;
- `$AttrDef` → Attribute info;
- `.` → Root directory;
- `$Bitmap` → Allocation status;
- `$Boot` → Boot Sector, BootCode;
- `$BadClus` → Cluster that have bad sector;
- `$Secure` → Security info;
- `$Upcase` → Uppercase version of every Unicode Character;
- `$Extend` → Application category;

18.4 Attibuti

18.4.1 Attribute Header

Descrive l'attributo (*tipo, dimensione,nome*):

- ID → identificativo univoco nell'entry (16 bit);
- Type ID → identificatore tipo attributo;
- OFFSet attribute Content.

18.4.2 Attribute Content

- Residente → viene posizionato all'interno della stessa entry;
- Non residente → viene posizionato in cluster esterni
  - **cluster run** → cluster consecutivi.

18.4.3 Standard Attribute Types

Definiti nel FS Metadata `$AttrDef`

16	$STANDARD_INFORMATION	*General information, such as flags; the last accessed, written, and created times; and the owner and security ID*
32	$ATTRIBUTE_LIST	*List where other attributes for file can be found*
48	$FILE_NAME	*File name, in Unicode, and the last accessed, written, and created times*
64	$VOLUME_VERSION	*Volume information*
64	$OBJECT_ID	*A 16-byte unique identifier for the file ordirectory*

80	$SECURITY_ DESCRIPTOR	*The access control and security properties of the file*
96	$VOLUME_NAME	*Volume name*
112	$VOLUME_ INFORMATION	*File system version and other flags*
128	$DATA	*File contents*
144	$INDEX_ROOT	*Root node of an index tree*
160	$INDEX_ALLOCATION	*Nodes of an index tree rooted in $INDEX_ROOT attribute*
176	$BITMAP	*A bitmap for the $MFT file and for indexes*
192	$SYMBOLIC_LINK	*Soft link information*
192	$REPARSE_POINT	*Contains data about a reparse point*
208	$EA_INFORMATION	*Used for backward compatibility with OS/2 applications (HPFS)*
224	$EA	*Used for backward compatibility with OS/2 applications (HPFS)*
256	$LOGGED_UTILITY_STREAM	*Contains keys and information about encrypted attributes*

18.5 `Base/Non-Base` MFT Entry

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

18.6 Sparse Attributes

Risparmiare di allocare cluster ZERO per l'attributo `$DATA`.

18.7 NTFS - Altre caratteristiche

- Compressione → gli attributi non residenti `$DATA`;
- Indicizzazione → collezione di attributi memorizzata in maniera ordinata (B-Tree).

18.8 File System Metadata `$MFT` File

Contiene la Master File Table → Cluster Iniziale (Boot Sector).

Layout → ≥ Windows 7 → cluster 786432 (0xC0000).

Entry[0] di MFT:

- `$DATA` → cluster usati;
- `$BITMAP` → stato di allocazione delle entry.

18.9 File System Metadata `$MFTMirr` File

Copia di backup della Master File Table. Prime 4 entry:

- `$MFT`;
- `$MFTMirr`;
- `$LogFile`;
- `$Volume`.

Entry[1] di MFT.

Layout:

- ≥ Windows 7 → dopo il Boot Sector (16° settore)
- < Windows 7 → a metà del file System.

18.10 File System Metadata `$Boot` File

Boot Sector:

- Dimensione dei cluster;
- Nr. di settori del File System;
- Layout MFT

  - Cluster iniziale;
  - Dimensione entry.

Entry[7] di MFT.

Layout → primi 16 settori del File System (Signatore → `0xAA55`)

18.11 File System Metadata `$Volume` File

Informazioni sul volume:

- Etichetta;
- Versione.

Entry[3] di MFT:

- `$VOLUME_NAME` → nome in UNICODE del volume
  - ID Type: 96;
- `$VOLUME_INFORMATION`
  - Versione di NTFS;
  - Dirty status;
- `$DATA` : 0 byte.

18.12 File System Metadata `$AttrDef` File

Definisce gli attributi:

- Nomi;
- Type ID.

Entry[4] di MFT.

18.13 File System Category - Analisi

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.

18.14 Content Category

Contenuto degli attributi:

- Residenti → all'intero delle entry MFT;
- Non residenti → cluster esterni.

Cluster:

- Cluster[0] = settore[0] del File System
  - *Settore* = *Cluster x* `Settori_Cluster`

18.15 File System Metadata `$Bitmap` File

Informazioni sullo stato di allocazione dei cluster:

- *Bit[x] = cluster[x]*
  - *Bit[x] = 1* → cluster x è allocato;
  - *Bit[x] = 0* → cluster x non è allocato;

Entry[6] di MFT.

18.16 File System Metadata `$BadClus` File

Traccia i cluster con settori danneggiati

Entry[8] di MFT:

- `$DATA` = «`$Bad`»;
- Flag = Sparse;
- Size = File System.

18.17 Content Category - Layout

Diverso a seconda della versione NTFS

Zona MFT:

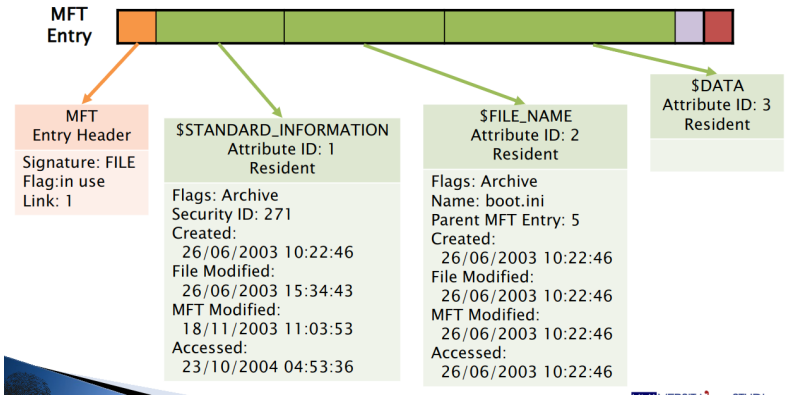
- Settori consecutivi riservati per MFT (`12,5%` del File System).

Boot Sector (Primo settore) → File System Metadata File dopo il Boot sector.

19 Lezione del 24-05 - L'analisi : I File System (pt4)

19.1 Metadata Category

Reperibili dagli attributi:



19.1.1 `$STANDARD_INFORMATION` Attribute

Esiste per ogni file e directory. Contiene i metadati principali:

- Informazioni temporali;
- Proprietà;
- Sicurezza e quota

Type ID → 16.

Byte	Descriptor	Es.
0-7	Creation time	NO
8-15	File altered time	NO
16-23	MFT altered time	NO
24-31	File accessed time	NO
32-35	Flags	NO
36-39	Maximum number of versions	NO
40-43	Version number	NO
44-47	Class ID	NO
48-51	Owner ID	NO
52-55	Security ID	NO
56-63	Quota Charged	NO
64-71	Update Sequence Number (USN)	NO

4 valori temporali (timestamp):

- Data di creazione;
- Data di ultima mdifica → modifica del contenuto degli attributi `$DATA` e `$INDEX`;
- Data di ultima modifica MFT → modifica dei metadati del file;
- Data di ultimo accesso.

19.1.2 `$FILE_NAME` Attribute

Ogni file e directory ha almeno un attributo `$FILE_NAME`. Dimensione di 66 byte + lunghezza nome.

Type ID → 48.

Riferimento al Parent Directory.

Namespace

0	POSIX: Il nome è case sensitive e permette tutti i caratteri Unicode eccetto per `/` e NULL
1	Win32: Il nome è case insensitive e permette la maggior parte dei caratteri unicode eccetto per alcuni come `/,\,:,>,<` e `?`
2	DOS: Il name è case insensitive, upper case e senza caratterisi speciali. Il nome deve avere altezza 8 o pochi caratteri nel nome e 3 o meno estensioni
3	Win32 & DOS: Usato quando il nome originale entra nel namespace DOS e 2 nomi non sono necessari

19.1.3 `$DATA` Attribute

Impiegato per memorizzare qualsiasi forma di dati:

- Non ha formato e valori Definiti

Presenta una dimensione ≥ 0 Byte. Con una dimensione maggiore di 700 byte → non residente.

Type ID → 128.

Alternative Data Stream (ADS) → attributi `$DATA` aggiuntivi.

19.1.4 `$ATTRIBUTE_LIST` Attribute

Lista degli attributi nella entry:

- Quando un `file/directory` necessita di più entry per gli attributi;
- Tipo di attributo → Posizione della entry che lo contiene.

Type ID → 32.

Byte	Descriptor	Es.
0-3	Attribute Type	YES
4-5	Length of this entry	YES
6	Length of name	YES
7	Offset to name (relative to start of this entry)	YES
8-15	Starting VCN in attribute	YES
16-23	File reference where attribute is located	YES
24	Attribute ID	YES

19.1.5 `$SECURITY_DESCRIPTOR` Attribute

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

Type ID → 80 (Solo versioni NTFS < 3.0)

19.1.6 File System Metadata `$Secure File`

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

Entry[9] di MFT:

- Indice `$SDH`;
- Indice `$SII`;
- Attributo `$DATA` (`$SDS`).

Ogni `file/directory`:

- `$STANDARD_INFORMATION` → Security ID (Indice nel `$Secure File`).

(Solo versioni NTFS < 3.0)

19.1.7 Algoritmi di allocazione

Allocazione delle entry MFT:

- Strategia del primo disponibile → dalla entry 24;
- Allocato → Non allocato (cambio della flag *in uso*);
- Non allocato → allocato (pulizia della entry).

Allocazione degli attributi:

- Riduzione dell'ultimo attributo (`$DATA`);
- Crescita dell'attributo
  - Residente → non residente.

19.1.8 Aggiornamento informazioni temporali

`$FILE_NAME`:

- Aggiornamento `creazione/spostamento` file.

`$STANDARD_INFORMATION`:

- Data di creazione (creazione di un file o copia);
- Data di ultima modifica → variazioen degli attributi DATA, `$INDEX_ROOT` o `$INDEX_ALLOCATION`;
- Data ultima modifica MFT → modifica degli attributi;
- Data di accesso → viene fatto accesso alla entry (metadati o contenuto).

19.1.9 Analisi

Individuazione di una entry MFT:

- Individuare la MFT tramite il boot sector.

Elaborazione del contenuto della entry:

- Elaborazione degli attributi:
  - `STANDARD_INFORMATION`;

  - `$DATA` (NON RESIDENTE → processare la RUNLIST);
  - `$FILE_NAME`.;

- Elaborazione delle possibili entry secondarie
  - `$ATTRIBUTE_LIST`.

19.1.10 File Name Category

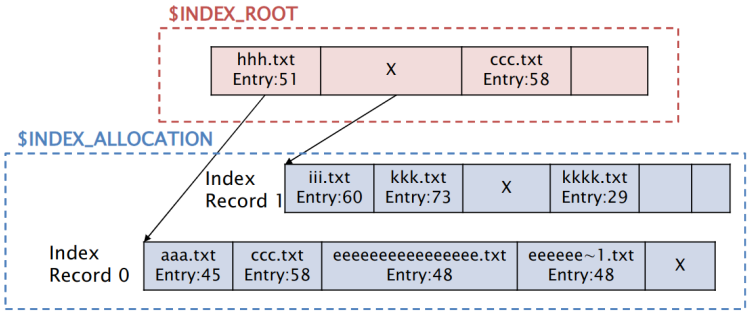
Correlazione dei nomi → Indici (racolta di strutture dati ordinate per chiave).

Struttura `B-Tree`:

- Nodi
  - `$INDEX_ROOT` (radice dell'albero);
  - `$INDEX_ALLOCATION` (indici utilizzati).

Directory Index Entry Data Structure

Byte	Descriptor	Es.
0-7	MFT file refernce for file name	YES
8-9	Length of this entry	YES
10-11	Lenght of `FILE_NAME` attribute	NO
12-15	Flags	YES
16+	$\text{FILE}_{\text{NAME}}$ = Attribute	YES
Last 8	VCN of child node in `INDEX_ALLOCATION`	YES



19.1.11 Root directory

Entry[5] di MFT → Nome «.»

Risiedono tutti i *File Syste Metadata File*.

19.2 Application Category

19.2.1 Disk Quotas (`$Quota`)

Supporto alle quote di spazio su disco:

- Limitare lo spazio allocato ad un utente.

Dati nel File System:

- NTFS < 3.0 → Entry[9] di MFT;
  - `\$Quota`
- NTF ≥ 3.0 → qualsiasi posizione di MFT;
  - `\$Extended directory`

Registro di Windows

19.2.2 `Logging/Journaling ($LogFile)`

Consente di mantenere il File System in uno stato di consistenza

Entry[2] di MFT

19.3 Analisi - File Recovery

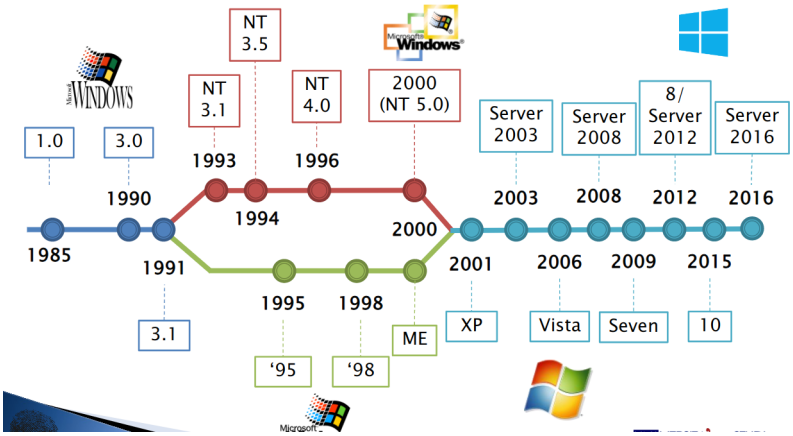
Eliminazione file:

- File name eliminato dall'index directory;
- Recupero entry MFT → attributo `$FILE_NAME` (Parent directory);
- Controllare la presenza di ulteriori `$DATA` (ADS).

20 Lezione del 26-05 - L'analisi : I Sistemi Operativi

20.1 Windows

20.1.1 Storia



20.1.2 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

20.1.3 Secure boot

Cerca di imporre il boot solo di Windows (per far partire altri sistemi è necessario disabilitarlo).

20.1.4 Registro di sistema

Impostazioni del SO e di Programmi installati.

Windows `95/98`:

- `User.dat`
  - `\Windows`;
  - `\Windows\Profiles\[user_name]`
- `System.dat`
  - `\Windows`

Windows $\geq$ XP

- Software, System, SAM, Security, Default:
  - `\Windows\system32\config`
- `NTuser.dat`
  - `\Documents and Settings\[user_name]` (Windows XP)
  - `\Users\[user_name]` (Windows $\geq$ Vista)

Struttura ad albero con 5 sotto-alberi principali (hive):

- `HKEY_CLASSES_ROOT`
  - Associazione $\rightarrow$ estensione file - applicazione
- `HKEY_USERS`
  - Impostazioni di tutti i profili utenti configurati nel sistema (`NTuser.dat`).
- `HKEY_CURRENT_USERS`
  - Puntatore al profilo utente presente in `HKEY_USERS` loggato nel sistema;
- `HKEY_LOCAL_MACHINE`
  - Configurazione del PC;
- `HKEY_CURRENT_CONFIG`
  - Punntatore alla corrente configurazione situata in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardwar` `Profiles\Current`

Ogni nodo dell'albero presenta:

- Chiave → coppia di valori (NomeChiave-Valore);
- Sottochiavi

20.1.5 Registro di sistema - Analisi

- Configurazioni dell'utente;
- Dispositivi USB;
- Informazioni temporali;
- Strumenti
  - RegEdit;
  - Windows Registry Recovery;
  - Registry Viewver (Access Data).

20.1.6 Thumbnails

Miniature delle immagini presenti nelle cartelle.

Windows 98 - XP:

- `Thumbs.db` → in ogni cartella in cui `sono/erano` presenti immagini.

Windows ≥ Vista:

- Database centralizzato `thumbcache_[NUM].db`
  - Dove *NUM* → dimensioni delle anteprime 96, 256, 1024.

Analisi → miniature di immagini non più presenti:

- Thumbs Viewer;
- Thumbcache Viewer.

20.1.7 ShellBag

Personalizzazioni utente delle visualizzazione del contenuto delle cartelle

Chiavi di registro:

- HKEY_USERS\<USERID>\Software\Microsoft\Windows\Shell\;
- HKEY_USERS\<USERID>\Software\Microsoft\Windows\ShellNoRoam (Windows < Vista);
- HKEY_USERS\<USERID>\Software\Classes\LocalSettings\Software\Microsoft\Windows\Shell\ (Windows ≥ Vista).

BagMRU → storico di tutte le cartelle visualizzate dall'utente.

Bags → impostazioni di visualizzazione delle cartelle contenute in BagMRU.

Per analizzare questi dati si segue la lista delle cartelle presenti in MRUListex:

- Si seleziona visualizza il valore ella chiave relativa → nome cartella
- Si segure la sottochiave della cartella (Si visualizza la chiave MRUListex e si continua ricorsivamente la sua esplorazione)

Informazioni ottenibili

- **Bag Number** → la sottochiave Bags che contiene le preferenze dell'utente (Nodeslot);
- **Registry Key last write time** → data di primo accesso o di ultima modifica della cartella;
- **Folder name** → nome della cartella.

Tool → ShellBagsView

20.1.8 Event Viewer

Sistema di *logging* standard (EVT/EVTX)

20.1.9 Application Data

Impostazioni dei programmi utilizzati dall'utente e file temporanei

Windows XP:

- \Documents and Settings\[nome_utente]\;
- Dati Applicazioni;
- Impostazioni locali.

Windows ≥ VIsta:

- \Users\[nome_utente]\AppData

20.1.10 Application Data - Analisi

Quadro complessivo dell'utilizzo del PC da parte di un utente:

- Posta elettronica;
- Cache;
- Cronologia;
- Log;
- Configurazioni.

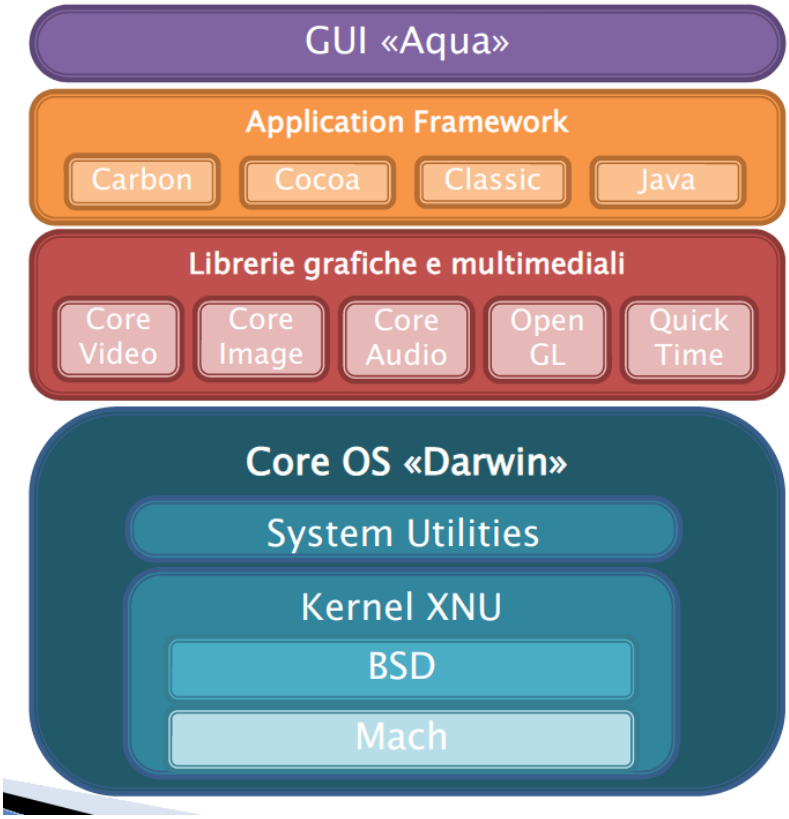
20.1.11 File Swap

Estensione della memoria volatile

20.1.12 Vantaggi e Svantaggi

Vantaggi	Svantaggi
Diffuso	Pochi log
Documentato (meh)	Presenza di antivirus che possono compromettere una timeline
Supportato (ti fanno buttare il sangue per il supporto)	Sistema commerciale

20.2 Apple OS `X/macOS`



20.2.1 Configurazione

NetInfo (DB ad oggetti):

- Controlla diverse configurazioni del SO
  - Entry statiche di rete (file hosts);
  - Definizioni di tutti gli utenti;

Gestione NetInfo:

- `/Application/Utility` (OS X $\leq$ 10.4)
- `/Application/Utility/Utility Directory` (OS X $\geq$ 10.4)

20.2.2 Configurazione server

Open directory (Mac OS X Server 10.4):

- Servizio di directory;
- Gestione delle autenticazioni;

Tool	Descrizione
dscl	Manipolazione e gestione dei servizi di directory
dsconfigldap	manipolazione degli alberi LDAP
dsconfigad	manipolazione dei sistemi Active Directory
dseditgroup	gestione di gruppi di utenti
dsenableroot	abilita/disabilita l'utente root in OpenDirectory
dscacheutil	regola le cache relative a OpenDirectory
dsmemberutil	Gestisce i gruppi di appartenenza di un oggetto OpenDirectory
dsexport	esporta oggetti da un albero OpenDirectory
dsimport	importa oggetti in un albero OpenDirectory

20.2.3 Cifratura

FileVault → cifratura della home directory (`/Users/[nome_utente]`).

FileVault 2 (OS X $\geq$ 10.7) → full disk encryption.

20.2.4 File swap

Estensione della RAM → `/private/var/vm/swapfile*`

Congelamento della memoria RAM in fase di sospensione → `/private/var/vm/sleepimage`

20.2.5 Portachiavi

Accentramento delle credenziali utente:

- Accesso tramite API;
- Cifratura AES-128.

OS X $\geq$ 10.9:

- Integrazione servizio Apple Icloud.

20.2.6 Analisi

Elevato numero di tecnologie proprietarie.

Strumenti:

- BlackBAg Technologies
  - Blacklight → toolkit forense;
  - MAcQuisition → tool di acquisizione forense;
- Mac Forensics Lab.

Apple hdiutil → tool da cli `c::`

- Apple DMG
  - Copia FullDisk;
  - Copia Logica.

20.2.7 Home Directory Utente

La granparte dei file dell'utente.

Dati delle applicazioni → `/USers/[nome_utente]/Library`

20.3 Gnu/Linux

Distribuzioni basate su kernel Linux

Linux Standard Base (LSB) → standardizzazione delle diverse distribuzioni

20.3.1 Componenti

- Kernel;
- Librerie di sistema;
- Tool di base.

20.3.2 Overview

(La parte delle slide del prof la salto perchè so tutte sbagliate `c:`)

20.3.3 Sistema

Multiutente e Multitasking. Struttura rigida del file system (in generale → discorso che non è valido per distribuzioni quali **NixOS** e **Guix**):

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 dl 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

20.3.4 Permessi di file e directory

- `r` → permesso di lettura;
- `w` → permesso di scrittura;
- `x` → permesso di esecuzione (file) e permesso di accesso (directory).

Per l'utente root invece non ci sono limiti sui permessi.

20.3.5 Log

Syslog → sistema di gestione Log:

- Presenta un demone (syslogd);
- Presenta una configurazione system-wide in `/etc/syslog.conf`

Facility code	Keyword	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authentication messages
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock daemon

Facility code	Keyword	Description
10	authpriv	Security/authentication messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	Log audit
14	console	Log alert
15	solaris-cron	Scheduling daemon
16-23	local0 - local7	Locally used facilities

Severity Value	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant conditions
6	Informational	Informational messages
7	Debug	Debug-level messages

La posizione dei log si trova nella directory `/var/log/`:

- **messages** → eventi relativi alla macchina;
- **wtmp** → registrazione degli accessi.

Logfinder → ricerca di tutti i file log

20.3.6 Home directory

Tipi di utenti:

- **root** → amministratore di sistema;
- **utente base**.

Directory disponibili per l'utente:

- `/usr/local/bin` → file dei programmi utilizzabili dall'utente;
- `/tmp` → directory di file temporanei;
- `/home/[nome_utente]` (sfruttando le variabili di ambiente → `$HOME`) → directory principale dell'utente
  - Dati dell'utente;
  - History della shell;
  - Cache → situata in `~/.cache`;
  - File di configurazione → situata in `~/.config` (eccetto per alcuni programmi che usano PATH diversi).

20.3.7 Directory `/var`

Contiene i dati che variano durante la normale esecuzione del sistema. Presenta:

- Log di sistema;
- Spool di stampa;
- Mail in transito e code;
- Tablespace degli RDBM;
- Cache di sistema;
- Configurazione dei vari tool;
- Database dei pacchatti installati;
- File di bind;
- Database di LDAP;
- Database di sistema di AFS;
- Database di Kerberos.

20.3.8 Analisi

Check su `inittab/systemd` (nel caso ovviamente la distro usi systemd come sistema di init).

Check sull'autenticazione (controllo sulla configurazione PAM, kerberos e openLDAP).

Controllo del montaggio dei file system all'avvio (in `/etc/fstab`)

21 Lezione del 31-05 - Mobile Forensic - Acquisizione e analisi

21.1 Overview

Vanno considerati una serie di fattori:

- Presenza di memorie diverse (interna ed esterna al dispositivo);
- Presenza di SIM CARD;
- Presenza di un `IMEI/MEID`.

21.2 `GSM/CDMA`

GSM → Global system for Mobile communications.

IMEI → codice univoco del dispositivo all'interno della rete mobile.

SIM Card:

- ICCID (Integrated Circuit Card ID) → numero seriale `19/20` cifre;
- IMSI (Interational Mobile Subscriber Identity) → identificativo nella rete mobile dell'operatore.

CDMA → Code Division Multiple Access.

MEID → Codice univoco del dispositivo all'interno della rete mobile (nessuna necessità di SIM Card).

21.3 Dispositivi

Android, IOS o altri (Jolla etc.)

21.4 Raccolta

Disabilitare tutte le connessioni:

- OFF Line mode `/` Airplane Mode;
- Faraday Bag;

L'obiettivo è evitare:

- Remote wipe;
- Sovrascrittura di informazioni presenti.

21.5 Sblocco del dispositivo

IOS (Max 10 tentativi):

- PassCode a 4 cifre;
- PassCode a 6 cifre;
- PassCode > 6 cifre;
- Password alfanumerica;
- `Face ID/ Touch ID`

Android (Max ? Tentativi):

- PassCode $\geq$ 4 cifre;
- Password alfanumerica;
- Pattern;
- `Face ID/ Touch ID`;
- Password di avvio.

Si cita anche come possibilità quella di protezione implementata dalle app (Applicazione di sicurezza).

Spesso lo spegnimento del dispositivo richiede un codice di sblocco

21.6 Sblocco della SIM Card

- PassCode a 4 cifre (PIN);
  - Max 3 tentativi
- PUK $\rightarrow$ recovery code
  - 8 cifre;
  - Max 10 tentativi.

21.7 Strumenti

Citiamo Cellebrite UFED (Universal Forensic Extraction Device).

21.8 Memory Card

Micro, Mini SD di diversi tagli:

- Presenza di Foto, Video, Musica;
- Presenza di Applicazioni;
- Presenza di Backup;
- . . . ;

È la prima cosa da acquisire (writeblock `hw/sw`).

21.9 SIM Card

(Mini, Micro, Nano, Full Size) SIM, con diversi tagli:

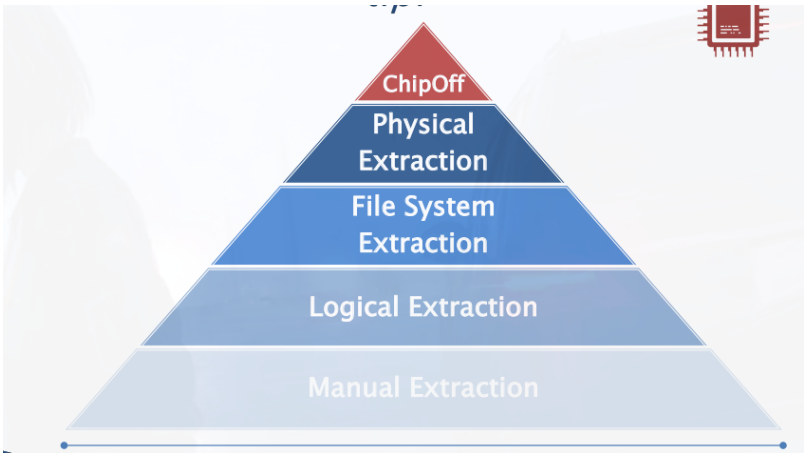
- Presenza di dati (Rubrica, SMS);
- Identificativi → ICCID, IMSI.

Struttura:

- Master File (root);
- Dedicated File (directory);
- Elementary File (file).

Acquisizione tramite Lettore di SIM Card

21.10 Tipi



21.10.1 Manual Extraction

Repertazione fotografica del contenuto (interagire con la GUI)

Svantaggi	Limiti
Processo lungo	Display non funzionante
Rischio `modifica/cancellazione` dei dati	Codice di sblocco
Visualizzazione limitata delle applicazioni	

21.10.2 Logical Extraction

Estrazione dei dati tramite API del dispositivo.

Limiti:

- I risultati dipendono dall'API
  - Parziali
    * Solo alcune informazioni di un dato;
    * Solo alcuni dati → nessun dato di app di terze parti;
- Codice di sblocco.

21.10.3 File System Extraction

Estrazione dei file tramite API del dispositivo.

Risultato:

- L'output va processato per visualizzare i dati contenuti
  - I Dati sono contenuti in DB SQLite;
  - Possibilità di visualizzazione dati cancellati (entry del DB).

Limiti:

- I risultati dipendono dai permessi con cui vengono fatte le richieste
  - File System Completo → tutta la struttura della live partition;
  - File System Parziale → solo determinate porzioni.

21.10.4 Physical Extraction

Copia bit-a-bit della memoira del dispositivo:

- Boot loader → codice immesso nella fase di avvio del dispositivo per avviare l'estrazione dati;

  - Bug del `firmware/Chipset`.

- Agent → tool installato nel SO (Bug nel SO);
- Advanced ADB (Android Debug Bridge) → Bug nel SO.

Risultato:

- L'output va processato per visualizzare i dati contenuti;
- Recupero di file cancellati (carving);

Limiti:

- Produttore del dispositivo;
- Chipset;
- Versione del SO;
- Patch di sicurezza.

21.10.5 Chip Off

Estrazione fisica del chip dalla scheda madre:

- Distruzione del dispositivo

Limiti → dispositivo cifrato.

21.11 Analisi

21.11.1 Sistemi operativi

OS Android:

- Migliaia di produttori e modelli;
- Kernel Linux → OpenSource;
- App.

IOS:

- Pochi modelli;
- Closed;
- App.

21.11.2 App

Estendono la funzionalità del SO

Rappresentao le principali interazioni con l'utente (produzioni di dati).

Hanno un proprio dominio.

22 Lezione del 07-06 - Fase finale - La Relazione tecnica

22.1 Descrizione e valutazioni

Parte descrittiva → dettagliata e accurata (documentazione fotografica)

Parte Valutativa → motivazioni, descrizioni dell'iter logico.

22.2 Forma

Quattro parti:

- Parte epigrafica → indicazione degli estremi del `P.P.`, PM, Giudice, descrizione dell'incarico, parti presenti ad un accertamento, etc;
- Parte descrittiva → illustrazione degli accertamenti `e/o` ricostruzioni compiuti;
- Parte Valutativa → risposta ai quesiti con motivazione esaustiva delle conclusioni;
- Parte Riassuntiva → esposizione sintentica della risposta ad ogni quesito;

Deve essere chiara e intellegibile → impiego di grafici, illustrazioni, tabelle, etc.