LEZIONE 2 - PROCEDIMENTO PENALE

Fasi del procedimento Penale:

Iscrizione notizia di reato: Quando le autorità giudiziarie ricevono una notizia di reato, il Pubblico Ministero (PM) iscrive la notizia.

Indagini Preliminari: Il PM e la PG svolgeranno le indagini per appurare che il reato sussista. Possono usare la perquisizione e il sequestro probatorio. Perquisizione cerca la prova, il sequestro probatorio la conserva per evitare alterazioni.

Accertamento tecnico: Il PM nomina un consulente tecnico per effettuare accertamento tecnico. ART 359.

Accertamento tecnico irripetibile: ART 360. Il PM esegue l'accertamento avvisando prima l'indagato e il difensore e poi la parte offesa e il difensore. Entrambe le parti possono assistere a tutta l'operazione. HANNO FACOLTÀ di nomina del Consulente tecnico di Parte.

Misure cautelari: Misure reali, limitano l'uso dei beni della persona, Misure Personali, limitano la libertà della persona.

Incidente Probatorio: Può essere richiesta dalle parti ed ha la funzione di anticipare la formazione e l'acquisizione di una prova. Viene richiesta al GIP. Il GIP Può nominare un Perito.

Richiesta di Archiviazione: Il PM può chiedere di archiviare il caso se: gli elementi non sono sufficienti per l'accusa, l'autore del reato è ignoto, il reato è estinto, il fatto non è reato, il fatto è particolarmente tenue. La parte offesa può opporsi notificando al GIP.

Rinvio a Giudizio: Il PM esercita l'azione penale e indica il capo di imputazione.

Udienza preliminare: Indagato diventa imputato, il GIP viene sostituito dal GUP, l'imputato può richiedere di essere prosciolto, e di rinunciare alla fase dibattimentale.

Fase dibattimentale: Si presentano le prove documentali e le testimonianze, c'è l'uso della perizia.

Sentenza: Proscioglimento o Condanna.

Impugnazione: Si passa alla corte d'appello 2 grado di giudizio e se necessario 3° grado Corte di cassazione.

Giudicato penale: La sentenza è irrevocabile ed immodificabile. L'imputato non può essere di nuovo sottoposto allo stesso procedimento penale.

LEZIONE 3 - GLI ATTORI DEL PROCEDIMENTO PENALE

Gli attori:

PM: Dirige le indagini preliminari e si avvale della PG, nomina Consulenti tecnici ed esercita l'azione penale.

PG: Forze di polizia che collaborano con il PM. Svolgono attività investigativa, informativa, prevenzione, assicurativa.

Persona Offesa/Attore-Ricorrente(Civile): è il soggetto leso dall'autore del reato. Ha il diritto di querela, può presentare memorie ed indicare elementi di prova. Può nominare un difensore e consulenti tecnici.

Indagato (dopo Imputato)/Convenuto-Resistente(Civile): Sono la stessa persona, cambia nome con il rinvio a giudizio. Ha l'obbligo di avvocato, e possono avvalersi di Consulenti Tecnici.

Avvocato Difensore: Si occupa della parte legale di entrambe le parti.

GIP: Funzione di garanzia dell'indagato nella fase delle indagini preliminare, può accogliere oppure no l'archiviazione, non ha iniziativa probatoria e si avvale dei registri del PM.

GUP: Ascolta le ragioni della difesa dell'imputato. Valuta le prove, può emettere il rinvio a giudizio oppure la sentenze di non luogo a procedere.

Giudice del dibattimento: Emette la sentenza, presiede a tutta la fase dibattimentale.

Computer Forenser: se sono richieste particolari competenze può essere nominato dal PM e dalla PG.

Il Ruolo del Computer Forenser:

Deve impiegare strumenti che garantiscono l'inalterabilità della prova anche se non dettagliatamente descritti dalla legge.

Accertamento tecnico irripetibile ART 360: Accertamenti che se compiuti comportano la fonte della prova e la ripetibilità della procedura non è garantita. Esigente di restituzione del reperto. Il PM in questa fase deve avvisare l'indagato e il suo difensore in modo da permettere di assistere a tutta la fase, possono nominare un consulente tecnico di parte.

Perito: In caso di incidente probatorio o di un'udienza in cui sono richieste capacità tecniche, il GUP può nominare un Perito.

I nomi del computer forenser: Ausiliario PG, CTU, CTP, Perito (del Giudice).

LEZIONE 4 - ORIGINE DEL REATO INFORMATICO:

Origini:

Reato informatico: è un reato in cui c'è un dispositivo informatico come strumento o come oggetto oppure illecito che richiede conoscenze informatiche.

Reato informatico nel Diritto: A livello internazionale si è rinunciato a dare una definizione di reato informatico. Si è preferito etichettare come reati alcuni comportamenti.

Esempi di comportamenti illeciti: Frode informatica, accesso abusivo ad un sistema informatico, danneggiamento di dati, informazioni oppure programmi informatici.

LEZIONE 6 - IDENTIFICAZIONE E RACCOLTA:

FASE 1: Identificazione.

Identificazione: individuare dove il dato è conservato (notebook, smartphone etc). Si effettua la **PREVIEW**, si esegue un'analisi di primo livello delle memorie del dispositivo. Si usa un **Write Blocker (SIA Software o Hardware)**. rischio di alterazione di prova.

Preview - Dead: Analisi con SO spento, richiede write blocker hardware oppure software. Pro - non altera il dispositivo e permette di utilizzare diversi software. Contro - buona conoscenza del sistema da analizzare, non praticabile su sistemi embedded (smartphone, router).

Preview - Live: Analisi eseguita ad SO acceso, Pro: è veloce nell'analisi dei programmi installati, c'è visione dell'ambiente utente. Contro: alterazione del reperto, uso di software compatibili al sistema. Non è obbligatorio il write blocker.

Shutdown del dispositivo: Se un dispositivo è acceso bisogna tenere in considerazione la cifratura, il software in esecuzione e il dump della RAM.

Accensione del dispositivo: Tenere in considerazione ultimo accesso al dispositivo e esecuzione su disco di diverse operazioni.

FASE 2: Raccolta.

Sequestro: Il dispositivo se contiene dati di valore si può effettuare il Sequestro Fisico (requisire fisicamente il dispositivo) oppure Sequestro Logico (copia totale o parziale del dispositivo).

- **Catena di custodia:** Si applica in caso di sequestro fisico, verbalizzare ogni cosa che può identificare il dispositivo. Non sempre praticabile in caso di dispositivi che non possono essere spenti o spostati.

Copia Forense: Garanzia di ripetibilità dei successivi accertamenti che verranno eseguiti sulla copia forense.

Acquisizione Fisica: Copia bit a bit dell'intero supporto di memoria.

Clonazione: ha come risultato un supporto pressoché identico a quello originale. E' facilmente alterabile, viene usato solo nei casi in cui bisogna metterlo nel proprio alloggio di funzionamento.

Acquisizione ISO: Generazione di file immagine, ha come risultato un file rappresentante il supporto originale. E' maneggevole e può essere usato per generare un disco clone.

LEZIONE 7 - VALIDAZIONE E PRESERVAZIONE:

FASE 3: Validazione. (garantisce che la copia eseguita è identica al supporto originale).

Copia forense: L'HASH è una stringa a lunghezza fissa che serve ad identificare una copia.

Garantisce che la copia effettuata sia identica al disco originale (avranno lo stesso HASH).

Copia Forense ART 360: Si deve effettuare quando le memorie non sono in buono stato, quando.

una copia viene fatta in "Live Acquisition" (Smartphone o server), oppure a causa del dissequestro.

FASE 4: Preservazione (garantisce che non vengano effettuate modifiche alla copia forense).

La preservazione garantisce che non vengano eseguite modifiche o alterazioni alla copia forense, se ciò avviene l'hash cambierà.

Comando DD: E' presente in quasi tutte le distro Unix. **/dev/sda** disco di origine - **/dev/sdc1** disco destinazione.

```
dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
```

Copia Corretta.

IF: input file(sda). **OF:** output file(sda.dd). **BS:** Default 512 bytes(ma ora 2048). **CONV =** Noerror,sync (va avanti finché non trova errori. sostituisce i blocchi non letti nella destinazione con NULs).

```
dd if=/dev/sda bs=2048 | split -d -b 2G - mnt/dest/dd_image/sda
```

SPLIT: divide il file immagine. -d, aggiunge un contatore alle parti. -b parti da massimo 2GB.

```
md5sum /dev/sda > /mnt/dest/dd_image/sda_orig.hash
cat /mnt/dest/dd_image/sda_orig.hash
```
Calcolo hash disco originale

```
md5sum /mnt/dest/dd_image/sda.dd > /mnt/dest/dd_image/sda_dd.hash
cat /mnt/dest/dd_image/sda_dd.hash
```
Calcolo Hash copia.

```
dd if=/dev/sda bs=2048 | tee /mnt/dest/dd_image/sda.dd |
md5sum > /mnt/dest/dd_image/ sda.hash
```
Copia e calcolo Hash insieme.

TEE: produce 2 stream, uno per la copia e lo stesso stream lo indirizza anche al calcolo dell'Hash.

```
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 su più file. **OFSZ:** dim massima file. **BUFSIZ:** è il block size. log Verb: log dettagliato.

LEZIONE 8 - DISK IMAGE:

Formati:

DD/RAW: E' un semplice container dello stream. Non conserva metadati, non conserva hash calcolati. Non esegue compressione. Massimo 1 file di flusso.

Expert Witness Disk Image Format (EWF): Formati più avanzati con capacità di segmentazione e dotati di più sezioni.

- **SMART:** Dotato di 4 sezioni e permette l'accesso veloce ad una parte dell'immagine.
- **Encase E01 BitStream:** 3 livelli di compressione. Dotato di 13 sezioni.
- **Encase L01 Logical:** Acquisisce file logici. Dotato di 15 sezioni.

Advanced Forensics Format (AFF/AFF4): Formato open source ed estensibile. Ogni disco viene separato in due strati, uno contiene i metadati, l'altro i dati effettivi.

Tool di Acquisizione:

Guymager: Open source su Linux, basato sulla libreria degli libEWF. Supporta img DD e EWF.

Supporta calcolo Hash di MD5 - SHA1 - SHA256. Fa uso della Hashing on the fly, copie full disk.

FTK Imager: Freeware su Windows. Supporta copie fisiche, logiche, di immagini, cartelle e di dvd multipli. Supporta i formati DD - SMART - E01 - AFF. Permette la segmentazione, la compressione e la crittazione. Permette il DUMP della memoria RAM.

LEZIONE 9 & 10: FUNZIONI HASH E CALCOLO DEL PADDING:

Funzioni hash:

MD4: 3 round da 16 operazioni, con un buffer a 4 word, 3 funzioni logiche, 2 costanti additive.

128 bit di buffer

MD5: 4 round da 16 operazioni, con un buffer a 4 word. 4 funzioni logiche, 64 costanti additive

ogni passo aggiunge il risultato del passo precedente. 128 bit di buffer.

SHA1: 160 bit di buffer, 80 costanti additive, ed è più sicuro e lievemente più veloce del MD5**.**

Calcolo del bit di Padding: Innanzitutto il calcolo del padding è uguale sia per MD5 che per SHA1.

Supponiamo di avere un messaggio di 980 bit, aggiungiamo ai bit del messaggio, la lunghezza in bit del messaggio che è 64 bit (valore fisso, è sempre uguale). Avremo 1044 bit (messaggio reale + lunghezza del messaggio). Ora dobbiamo trovare il prossimo multiplo di 512 più grande della lunghezza del messaggio. 512 < 1044 -> 1024 < 1044 -> 1536 > 1044. Il valore adatto è 1536, a questo si sottrae il valore del messaggio + la lunghezza del messaggio (calcolata precedentemente) ovvero 1044. Perciò 1536 (sarebbe 512 * 3) - 1044 = 492. 492 sono i bit di padding. M' (lunghezza del messaggio + messaggio espresso in bit + padding) = 1536 bit.

LEZIONE 12 & 13 - L'ANALISI:

Montare un file Immagine: montare un file immagine è un processo veloce e che non richiede software "forensics oriented" ma ha delle limitazioni, vengono visualizzati solo i file residenti e il riconoscimento del FileSystem è demandato al nostro S.O.

FTK Imager: permette l'analisi della copia forense, permette la perquisizione sia Dead che Live. E' il software che supporta più formati d'immagine, più supporti fisici e FileSystem.

Strumenti software: I **toolkit** supportano tutta la fase di analisi (AccessData FTK, Autopsy).

Forensic ToolKit (FTK): E' un software commerciale disponibile su Windows, supporta quasi tutti i file immagine, supporta quasi tutti i FileSystem (vedere slide per la lista - lunga-).

Autopsy: E' un software free e opensource multipiattaforma , supporta SOLO i seguenti file immagine (Encase E01, RAW "DD, BIN, IMG" e i Virtual Disk VMDK). Supporta quasi tutti i FileSystem.

Entrambi i software sono chiamati **ToolKit:**

La peculiarità dei **ToolKit** è che offrono più visualizzazioni delle informazioni contenute nella copia

forense.

Hanno una rappresentazione gerarchica dei file.

Permettono una **Catalogazione** per tipo, utilizzando un offset detto signature, serve a definire il formato.

I file vengono **Classificati**, ovvero arricchiti di attributi, come la Bad Extension oppure il Delete File, ovvero estensione sconosciuta oppure file cancellati dal file system.

Known File: i file possono essere confrontati per Hash, e, possono essere catalogati come Notable File (file importanti) oppure Ignorable File (file non importanti).

Analisi del contenuto dei File: è possibile estrarre dai file delle informazioni. Gli Artefatti. **Artefatti:** I metadati di un file (informazioni aggiuntive di un file)**,** visualizzazione degli allegati email, estrazione di informazioni dell'ambiente di lavoro (windows), lo user activity. La navigazione Web, l'Image/Video Gallery, il File Carving. E' possibile fare anche ricerche semi manuali come l'estrazione di documenti (Document Content) oppure ricerche sul testo (Autopsy Solr oppure FTK dtSearch).

LEZIONE 14 & 15 - AUTOPSY:

Autopsy è un software modulare, permette l'utilizzo Multi User, è dotato di una GUI funzionale ed è possibile ampliare le sue funzionalità creando gli Ingest Modules (Python o Java). Esso è dotato di:

Central Repository: è un database in cui vengono memorizzate le informazioni di casi precedentemente analizzati, è possibile evidenziare i casi come Notable o Ignorable File.

Formati supportati: Encase E01, RAW. I volumi DOS GPR MAC BSD SOLARIS. Ed i principali FileSystem.

GUI: La gui è strutturata in:

Evidence Tree, Views, Results, Tags, File List, Viewer.

Ad ogni file è possibile assegnare uno S (notable file) C (commento) O (occorrenze).

Ingest Modules: sono dei plugin responsabili di analizzare i dati presenti all'interno del file immagine. Di seguito i nomi degli Ingest Modules più importanti:

Hash Lookup: calcola l'hash MD5 di ogni file, lo memorizza nel Case DB, ricerca gli hash calcolati all'interno di una Known Hash e lo flagga come Notable oppure Ignorable File.

File Type: determina il tipo del file analizzando la signature. Il tipo viene conservato nel

Case DB. E' basato sulla Libreria Tika**.** Fa anche il controllo sulla Bad Extension.

File Extension Mismatch: confronta l'estensione di ogni file con la propria categoria di appartenenza, se le informazioni non sono coerenti viene etichettato. (Dipende dal modulo File Type). Serve a trovare i file che l'utente ha tentato di nascondere.

Exif Parser: estrae i metadati dai file JPEG, serve ad identificare la fotocamera, il timestamp dello scatto, e la geolocalizzazione dello scatto.

Embedded File Extractor: estrae i file contenuti negli archivi, i risultati si trovano nella tree view. Sono flaggati se protetti da password.

Email Parser: ricerca ed analizza gli archivi di posta elettronica.

Interesting Files: etichetta file e cartelle che si pensa possano essere interessanti, come backup, immagini di virtual machines, client cloud etc.

Encryption Detection: etichetta file e volumi che potrebbero essere cifrati.

Plaso: tool open source per eseguire il parsing di file log o per estrarre timestamp.

Virtual Machine Extractor: analizza le VM all'interno del reperto. Ricerca i file VMDK e VHD, viene creata una copia locale e successivamente vengono inseriti nei datasources.

Data Source Integrity: calcola e valida l'hash del reperto. Recupera l'hash dai metadati del disk image, calcola l'hash del disk image, e se fallisce la validazione invia alert.

Recent Activity: analisi del cestino(Recycle Bin), del Web Browser, analisi dei registri

(RegRipper). Il risultato si trova in Extracted Content.

Keyword Search: ricerca sul testo, grazie al motore Apache Solr e Apache Tika.

Correlation Engine: ricerca dei file del caso all'interno del Central Repository. Correla il caso corrente con i casi passati.

PhotoRec Carver: controlla nella memoria non allocata se ci sono file cancellati. I risultati si troveranno nella vista $CarvedFile.

Android Analyzer: analizza dispositivi Android ed app di terze parti. Estrae i registri di chiamate, contatti, messaggi, browser, geolocalizzazione, messaggistica.

Tagging: serve a creare un riferimento ad un file/item di interesse, è possibile commentare e sono associati ad un esaminatore. Si ritrovano facilmente file di interesse e sono facilmente esportabili nel report. **Selezione file di interesse solo tramite i tag**

LEZIONE 16 - I VOLUMI:

FASE 5 - L'Analisi:

Nei dischi, abbiamo il **Volume** che è un insieme di settori atto a memorizzare i dati. La **Partizione** è un insieme di settori che fanno parte di un volume ed il **Volume System** è colui che gestisce i volumi e le partizioni affinché esse possano operare come un unico grande disco. I **Volumi** hanno gli indirizzi:

- **Physical Address (LBA):** è l'indirizzo del settore calcolato in base al primo settore del disco.
- **Logical Disk Volume Address:** questo indirizzo punta al primo settore di un volume.
- **Logical Volume Partition Address:** questo indirizzo punta al primo settore della partizione.

DOS Partition:

Il sistema DOS è il partizionamento più comune. E' dotato di:

- **MBR (Master Boot Record):** primo settore è da 512 byte
  - E' dotato di boot code
  - E' dotato di una **Partition Table** con **4 entry**.
  - E' dotato di **Flag.**
  - Ha signature 0x55AA.

Il DOS è dotato di:

- **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 (logico).
- **Secondary Extended Partition**
- **etc**

TLDR: In pratica il MBR è può avere ufficialmente 4 partizioni primarie, per poter creare delle altre partizioni, bisogna trasformare una delle primarie in Extended partition, così all'interno è possibile creare delle partizioni logiche.

Il **Boot Code** è situato nei primi 446 byte del primo settore del MBR, serve ad identificare la

partizione di avvio tramite il **flag "bootable".** Il settore del MBR viene allocato all'inizio di ogni

Extended Partition.

Apple Partition Map:

Gli APM vengono usati soprattutto in sistemi vecchi non basati su processori Intel.

Non hanno limiti di partizioni

Gestisce volumi fino a 2TB.

GUID Partition Table:

Sistema moderno di partizionamento usato da EFI.

Supporta fino a 128 partizioni, ed è dotato di 5 aree/sezioni:

- **Protective MBR:** DOS Partition Table (1° sezione)
- **GBT Header:** definisce il layout delle aree.
- **Partition Table:** ogni entry descrive la partizione.
- **Partition Area:** locazione riservata alla partizione
- **Backup Area:** copia di backup del GTP Header e della Partition Table.

LEZIONE 17 & 20 - I FILE SYSTEM:

I file system permettono un'organizzazione gerarchica dei dati, organizzandoli in file e cartelle, così da poterli ritrovare velocemente.

I dati vengono suddivisi in:

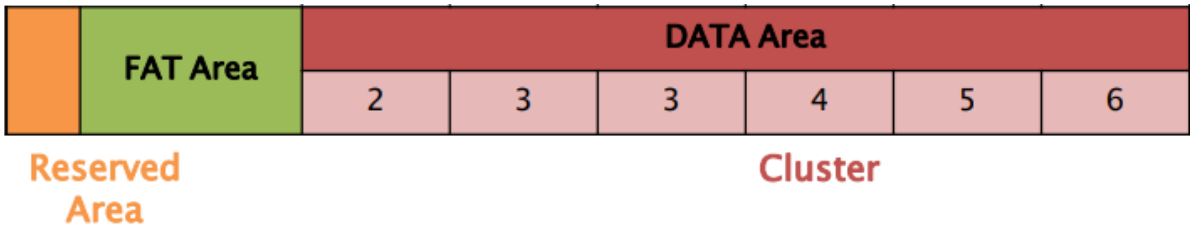
- **Dati essenziali:** che se modificati causano un malfunzionamento del sistema. (Indirizzamento del contenuto, nome del file, dimensione del file). **TRUSTED DATA**
- **Dati non essenziali:** informazioni accessorie, dati temporali. **UNTRUSTED DATA.**

Il **File System** si suddivide in:

- **File System Category:** troviamo informazioni generali sul file system, il layout dei dati e il controllo sulla consistenza - **volume slack -**
- **Content Category:** si occupa della memorizzazione dei file. E' suddiviso in **Data Unit** e può essere allocato o non allocato. L'allocazione del data unit può avere diverse strategie. "Primo disponibile" si cerca una data unit libera ogni volta partendo dall'inizio del file system. "Prossimo Disponibile" si cerca una data unit libera partendo dall'ultima allocata fino alla fine. "Del più adatto" si cerca in tutto il file system delle data unit libere consecutive che possano ospitare tutto il file. Nel content category si possono effettuare anche la ricerca di settori noti (Data unit view), ricerca di un contenuto specifico nei data unit (Logical file system searching), lo stato di allocazione dei data unit (data unit allocation status) ed il consistency check, ovvero ricerca dei data unit non referenziati in metadata category.
- **Metadata Category:** contiene la descrizione dei file presenti nel **content category**, come le informazioni temporali, o l'indirizzo di memoria di un file all'interno del data unit (**logical file address).** Lo **Slack Space** è la parte di data unit allocata ma non utilizzata. Nei metadata fanno parte anche i **Compressed File**, ovvero file dotati di compressione dei dati (mp3, jpeg), file compressi in archivi (zip, rar) oppure file compressi dal FileSystem.

- **File Name Category:** contiene il nome assegnato a ciascun file e l'indirizzo della struttura del metadato.
- **Application Category:** dati non più essenziali al file system. Il Journaling serve ad effettuare il rollback ad una modifica precedente del sistema. In analisi serve per ricostruire eventi di un incidente recente.

FAT File System:



Quando parliamo di file system FAT, noi abbiamo 3 versioni, FAT12 - FAT16 - FAT32. Il FAT12/16 non sono distinguibili l'uno dall'altro. Mentre il FAT32 ha un file aggiuntivo, il FSINFO, contenente la quantità di Cluster liberi e l'indirizzo del prossimo cluster libero.
I FAT sono dotati di Boot Sector, esso si trova nel settore 0 all'interno della Reserved Area. La dimensione della Reserved Area è di 1 settore per FAT12 e 16 mentre ha lunghezza variabile per la FAT32. Dopo la Reserved Area abbiamo la FAT Area e successivamente la Data Area, dove avremo i Cluster.
I Cluster partono dall'indirizzo 2 (Cluster#0 e #1 non esistono) e si trovano SOLO nella Data Area, essi contengono i file e le directory. Le entry (Fat12-fat16-fat32) sono uguali ai Cluster (entry[2] == cluster#2). L'entry[0] rappresenta l'informazione del media, entry[1] rappresenta il dirty status.
Un Cluster non allocato è uguale 0. Un cluster allocato invece, contiene il file più l'indirizzo del prossimo cluster. Un cluster allocato ha indirizzo del prossimo cluster oppure EOF 0x0fff fff8, invece un cluster danneggiato ha indirizzo 0x0fff fff7.

NT File System:

E' un file system sviluppato da Microsoft nel 1993. Al suo interno ogni cosa è rappresentata come un **FILE**

- **$MFT:** Master File Table, contiene le informazioni su tutti i file e directory di un volume NTFS. E' l'elemento principale di una partizione NTFS ed è rappresentato con la entry[0]. Contiene il cluster iniziale Boot Sector ed opera insieme alla $Data che tiene traccia dei cluster usati e alla $BitMap che controlla lo stato di allocazione delle entry.
- **$MFTMirr:** Contiene la copia di Backup delle prime 4 entry, ovvero di $MFT, $MFTMirr, $LogFile e $Volume. E' rappresentata dalla entry[1].
- **$LogFile:** contiene il Journaling. entry[2]
- **$Volume:** entry che contiene le informazioni sul volume, etichetta e versione. entry[3]
- **$AttrDef:** entry che tiene traccia delle informazioni sugli attributi (Nomi e Type ID). entry[4]
- **$Bitmap:** file che tiene traccia delle informazioni di allocazione dei cluster all'interno del volume. entry[6].
- **$Boot:** file che contiene il Boot Sector, informazioni sulla dimensione dei cluster, nr. settori del file system e contiene il layout dei primi 16 settori. entry[7].

Content Category:

Il **$Data** tiene conto della dimensione degli attributi, se l'attributo è <700 bytes il dato è residente e quindi interno al MFT, altrimenti non è residente. Se non è residente si salva un puntatore a cluster esterni.

Il **$BitMap** tiene conto dell'allocazione dei Cluster. I cluster allocati hanno valore 1, i non allocati 0.
Il **$BadClus** traccia i cluster con i settori danneggiati, si richiama con la entry[8] di MFT.
Metadata Category:
$Standard_Information esiste per ogni file e directory, al suo interno troviamo i metadata principali quali informazioni temporali e le proprietà.
$File_Name ogni file e directory ha almeno un attributo di questo tipo. Dimensione Fissa di 66 byte + lunghezza del nome.
Application Category:
Si occupa del logging/journaling ($LogFile), serve a contenere il file system in uno stato consistente. entry[2] di MFT.

LEZIONE 21 - SISTEMI OPERATIVI:
Microsoft Windows: e' un sistema operativo dotato di una sezione **Users** che si occupa dell'accesso al sistema. Gli account utente possono essere ad accesso locale, account di dominio oppure tramite autenticazione online.
Windows è caratterizzato da un registro di sistema che si occupa di mantenere salvate le impostazioni del sistema operativo e dei programmi installati. Ha una struttura ad albero con 5 sotto-alberi:

- **HKEY_CIASSES_ROOT**: si occupa delle estensioni dei file e delle applicazioni.
- **HKEY_USERS:** troviamo le impostazioni di tutti i profili utente configurati nel sistema.
- **HKEY_CURRENT_USER:** mantiene il puntatore nel **HKEY_USER** al profilo appena loggato nel sistema.
- **HKEY_LOCAL_MACHINE:** contiene la configurazione del computer.
- **HKEY_CURRENT_CONFIG:** mantiene il puntatore alla configurazione corrente situata in HKEY_LOCAL_MACHINE**.**

La maggior parte delle informazioni utente sono conservate nel registro di sistema. Ha una gestione della struttura del file system poco rigida. Grazie al pagefile.sys (swapfile) è possibile estendere la dimensione della memoria RAM, essa si trova nella Root del disco (a differenza di Apple). I file utente si trovano all'interno del registro. Windows ha un "event viewer" che si occupa della gestione dei Log, è dotato di Thumbs che sono delle miniature di immagini presenti nelle cartelle, grazie a Thumbs Viewer e a Thumbcache Viewer è possibile recuperare miniature di immagini non più presenti. E' dotato anche di una (Shell Bag) BagMRU che tiene traccia dello storico delle cartelle visualizzate dall'utente, e di Bags che rappresenta le informazioni di visualizzazione delle cartelle. Windows è il sistema più documentato, diffuso e supportato. Però ha pochi log ed essendo molto diffuso è più soggetto a virus.
Apple OS X: è un sistema operativo dotato di un sistema di cifratura full disk chiamato FileVault. Lo swapfile (pagefile.sys) è contenuto all'interno del percorso /private/var/vm/swapfile, mentre il la sospensione all'interno del /private/var/vm/sleepimage.
La gran parte dei file dell'utente si trova all'interno della **Home Directory,** mentre i dati delle applicazioni si trovano all'interno della **Library.**
Linux: e' dotato di Kernel, Librerie di sistema e di Tool di base. E' un sistema multitasking e multiutente dotato di una struttura del file system rigida. Linux produce un grande numero di log.
Linux ha diverse directory tra cui la **/home/nomeutente** dove troviamo i dati dell'utente, la **shell history** (i comandi usati dall'utente), la cache e i file di configurazione. La **/tmp** dove

troviamo i file temporanei. **/usr/local/bin** è dove si trovano i programmi utilizzabili dall'utente. **/var** contiene i dati che variano nel tempo, come i log di sistema. L'analisi di un sistema linux si esegue su /home, /etc e su /var.

LEZIONE 22 - MOBILE FORENSICS:
La connettività della mobile forensics consiste in 2 tecnologie principali:

- **GSM:** dotata di un IMEI, codice univoco del dispositivo all'interno della rete mobile. Dispositivo dotato di SIM card contenente un ICCID (serial number della sim) e il IMSI identificativo all'interno della rete dell'operatore.
- **CDMA:** protocollo che non consiste nell'uso della SIM card in quanto il dispositivo si trova già all'interno della rete di una rete mobile identificato mediante un MEID.

Quando dobbiamo analizzare un dispositivo mobile bisogna:

- Disabilitare le connessioni attivando la modalità aereo, per evitare un remote wipe.
- Sbloccare il dispositivo, nel caso fosse protetto da password i protocolli cambiano in base al sistema operativo (Android - iOS).
- Spegnere il dispositivo.

Acquisizione - Gli strumenti:
Le cose di maggior valore da acquisire da un dispositivo mobile sono:

- **Memory card:** contengono foto, video musica, applicazioni o backup.
- **SIM card:** contengono rubrica, sms, identificativi e sono dotati di una struttura root con directory e file.

Acquisizione - Tipologie:

- **Manual Extraction:** è una repertazione fotografica della GUI del dispositivo, è un processo lungo, ha il rischio di cancellare/alterare i dati e ha una visualizzazione limitata delle informazioni. Non è praticabile in caso di schermo rotto o codice di sblocco attivo.
- **Logical Extraction:** estrazione tramite API del dispositivo. I risultati ottenuti saranno parziali, non estrae dati da app di terze parti. Non praticabile in caso di codice di sblocco.
- **File System Extraction:** estrazione tramite API del dispositivo. Da un file in output che va processato in un DB SQLite. Permette la visualizzazione di dati cancellati. Il risultato dell'estrazione dipende dai permessi ottenuti, se il file system è completo, avremo dati completi altrimenti solo determinate porzioni saranno disponibili.
- **Physical Extraction:** Copia bit a bit della memoria del dispositivo utilizzando il boot loader. Il tool utilizzato è il comando ADB. L'output ottenuto andrà processato per visualizzare il contenuto. Potenzialmente otteniamo tutta la memoria del dispositivo, compreso i file cancellati, ma possono presentare dei bug che dipendono dal produttore del dispositivo, dal chipset, dalle patch di sicurezza, dal SO etc.
- **Chip:** estrazione fisica del chip dalla scheda madre, questo porta alla distruzione del dispositivo. Se il dispositivo è cifrato è inutile farlo.

Le App rappresentano il modo di interfacciarsi con il cellulare per poter utilizzare alcune funzionalità. Sono un ottimo modo per la produzione di dati.
Lo strumento da poter utilizzare per analizzare un dispositivo mobile è **UFED Physical Analyzer**. E' un software modulare che permette di poter essere ampliato nelle potenzialità.