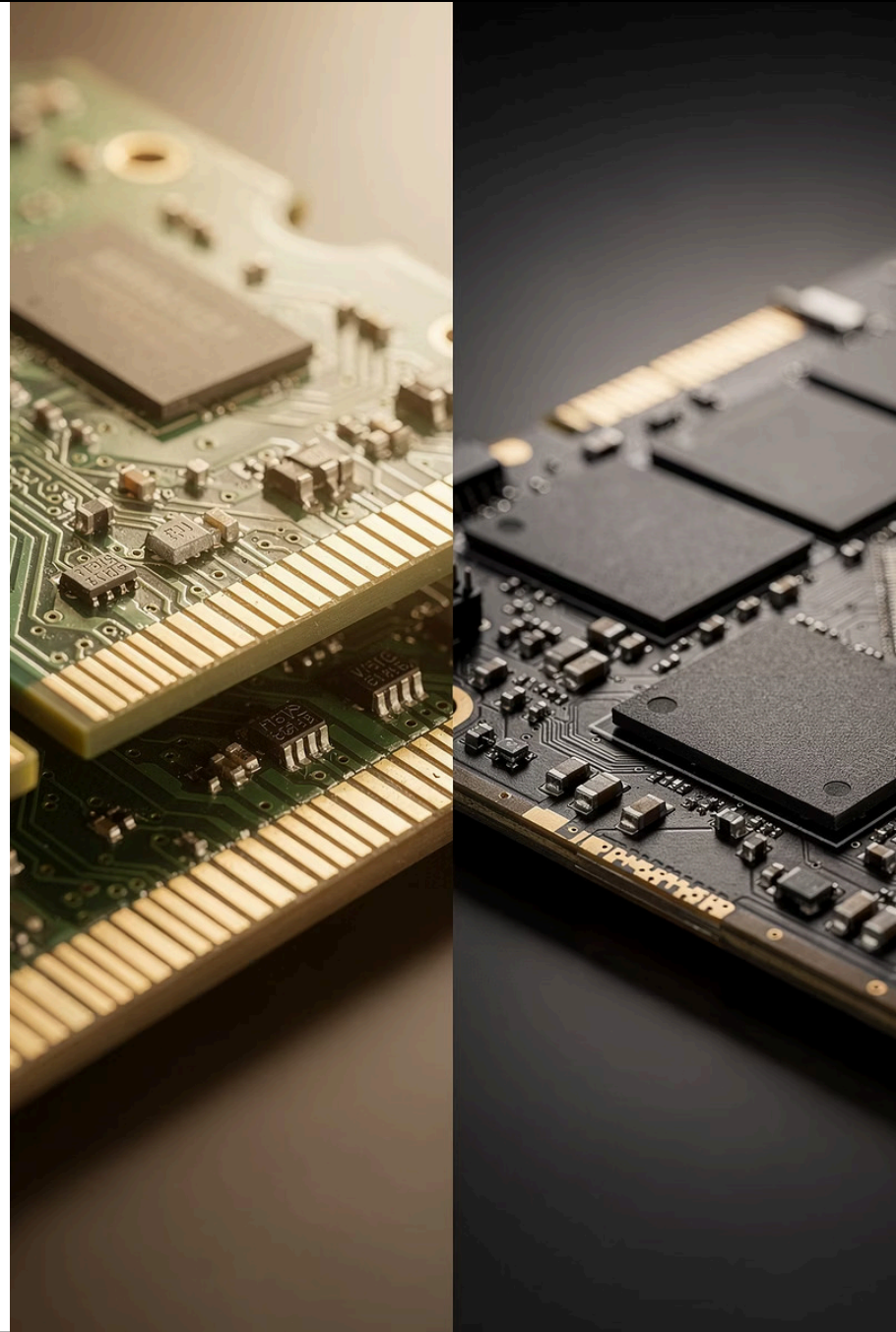
Acquisizione,custodia e analisi forense dei supporti di memoria

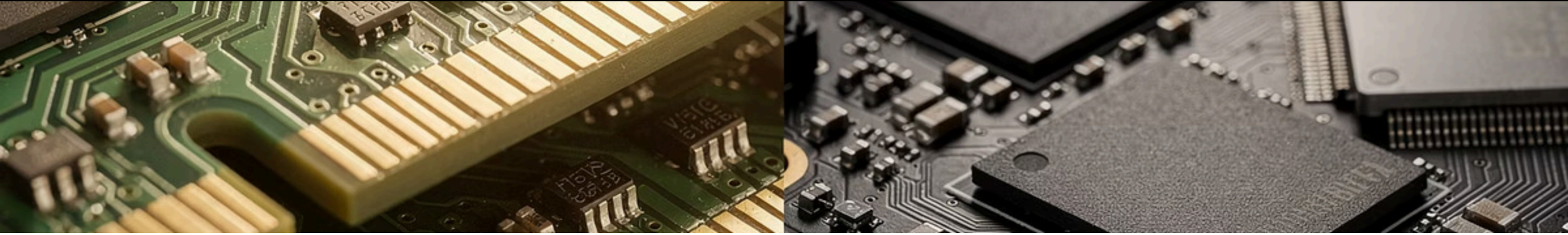
Ordine degli Ingegneri della Provincia di Palermo

Seminario "*Informatica forense*"

Palermo, 2 Aprile 2026

Relatore ing. Emanuele Cipolla
<emanuele@emanuelecipolla.net>





Memorie Persistenti e Non Persistenti

💾 Memorie Persistenti

Conservano i dati senza alimentazione — ideali per analisi post-mortem

HDD

Hard Disk Drive tradizionali

SSD

Solid State Drive ad alta velocità

USB / SD

Dispositivi di archiviazione esterni

Ottici

CD, DVD, Blu-ray

Memorie Non Persistenti

NON conservano dati volatili persi allo spegnimento — richiedono acquisizione "live"

RAM

Memoria di lavoro

Cache CPU

Memoria ultra-veloce all'interno del processore

Registro Attivo

Informazioni temporanee del sistema operativo

Connessioni Rete

Dati in transito o sessioni aperte

Conservazione dei reperti informatici

I reperti informatici devono essere conservati garantendone **integrità e inalterabilità nel tempo**, con attenzione alla **non modificabilità** dei metadati e dei timestamp originali.

(Alcuni) riferimenti normativi e *best practices*

- Artt. 259, 260 c.p.p.
- Direttiva UE 2016/680
- Standard ISO/IEC 27037:2012
- Linee guida SWGDE
- Best Practices ACPO v5.0

La Catena di Custodia

La catena di custodia traccia la raccolta, il controllo, il trasferimento e l'analisi delle prove digitali.

Chi

Ogni persona che ha gestito la prova deve essere documentata con nome e ruolo

Quando

Data e ora di raccolta o trasferimento devono essere registrate con precisione

Perché

Il motivo di ogni trasferimento deve essere esplicitato nella documentazione

Procedura Standard

1

Salvare i materiali originali e fotografare le prove fisiche

2

Fare screenshot delle prove digitali e **documentare data/ora**

3

Creare un clone e verificare con hash test

Se la catena di custodia non viene mantenuta ci si apre a **contestazioni e rischi di inammissibilità.**

Custodia e Conservazione dei Supporti

Contenitori Certificati

Buste antistatiche sigillate con etichetta antimanomissione e codice identificativo univoco per ogni reperto

Ambiente Controllato

Temperatura 18–22°C e umidità relativa 40–60%. Condizioni stabili per preservare l'integrità fisica dei supporti

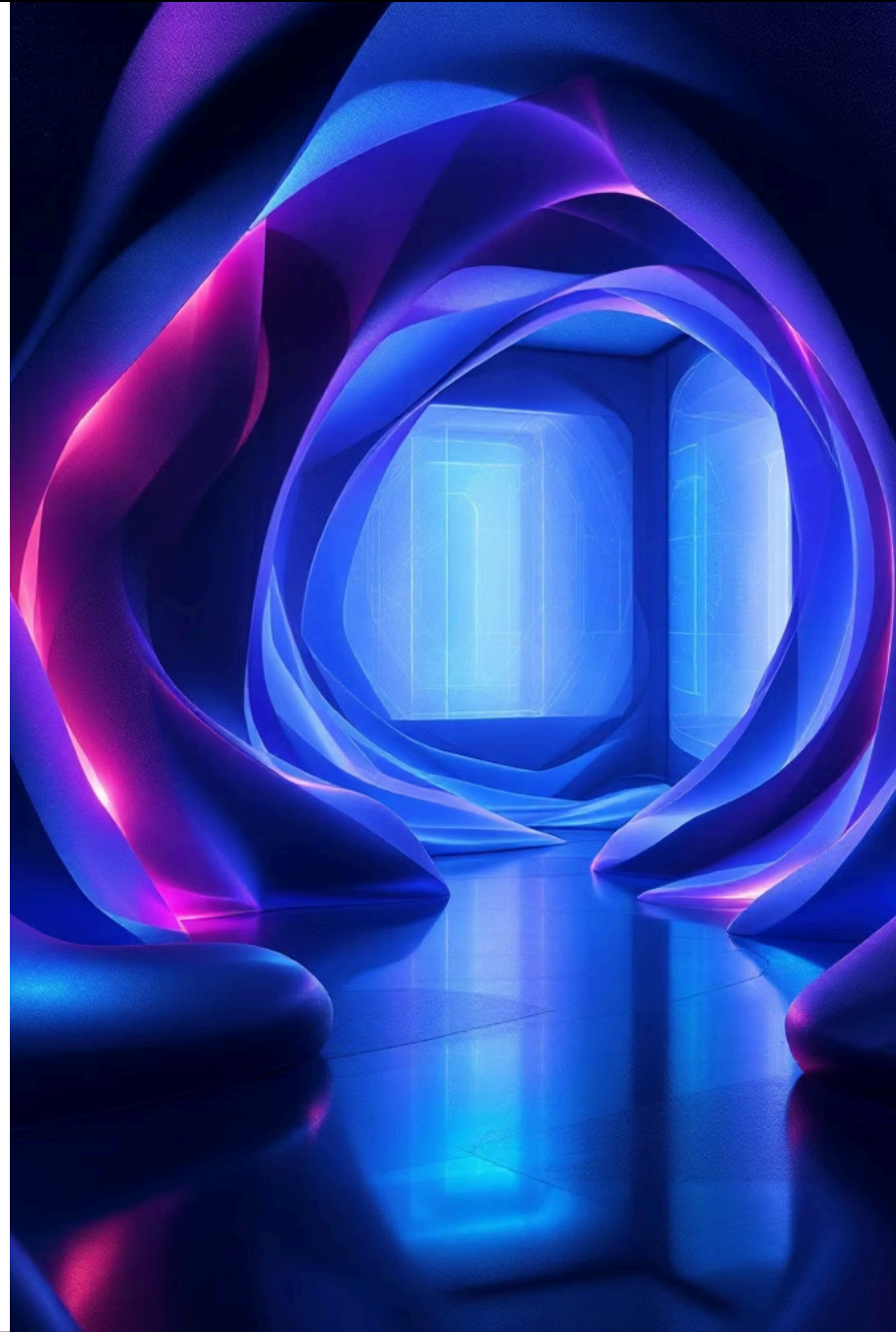
Protezione EM

Gabbie di Faraday o armadi schermati certificati ISO 27037 per protezione da campi elettromagnetici

Controllo Accessi

Sistemi biometrici con registrazione automatica e CCTV. Backup periodici con verifica hash trimestrale

SSD e dispositivi con batteria interna: regime di verifica aggiuntivo ogni 90 giorni con documentazione fotografica e nuova verifica hash. Per supporti danneggiati: imaging a freddo in camera bianca certificata ISO 14644-1.



(Alcuni) errori possibili nella Catena di Custodia

Lavorare sull'originale

Lavorare sulla sorgente dati originale anziché su una copia secondaria modifica inevitabilmente i dati — anche un semplice accesso a un file ne cambia le proprietà.

Write-blocker software inaffidabili

I write-blocker software sono notoriamente inaffidabili: possono fallire nel bloccare le scritture. Preferire sempre soluzioni hardware.

Dispositivo ricevente non sterilizzato

Dimenticare di sterilizzare il drive ricevente prima di clonare: possono emergere artefatti da casi precedenti recuperabili via carving.

Dispositivi trasmittenti lasciati attivi

Lasciare attivi dispositivi trasmittenti (cellulare, WiFi, Bluetooth) senza gabbia di Faraday invalida la catena di custodia.

Workstation investigatore sbloccata

Lasciare il computer dell'investigatore sbloccato può potenzialmente invalidare tutte le prove raccolte.

Fonte: ***Belkasoft — "Preserving chain of custody in digital forensics"***

Per un buon sopralluogo

1 **Non alterare l'integrità**

Le azioni per raccogliere e mettere in sicurezza le prove digitali non devono alterarne l'integrità in alcun modo

2 **Personale formato**

Le persone che esaminano le prove digitali devono essere specificamente **formate** a tale scopo

3 **Documentazione completa**

Ogni attività relativa a sequestro, esame, conservazione o trasferimento deve essere documentata e disponibile per la revisione

Concetti-chiave

Inventario

Identificare numero e tipo di computer, determinare se è presente una rete

Interviste

Intervistare, se necessario, l'amministratore di sistema e gli utenti presenti

Documentazione Media

Identificare e documentare tipi, volume e posizione dei media in esame

Archiviazione Remota

Identificare aree offsite, postazioni remote e software proprietario

Fonte: Infosec Institute

Workflow

🔌 1. Preparazione

Collegare dispositivo di test tramite write-blocker **hardware**

(nel caso di acquisizioni statiche)

📀 2. Acquisizione

Salvataggio **accurato** del contenuto attuale della memoria e delle **tracce** del contenuto passato

✅ 3. Verifica

Osservare calcolo hash e report finale di integrità

🔍 4. Analisi

Estrarre le informazioni rilevanti per il quesito posto

Strumentazione Forense

🔒 Write-Blocker

Dispositivo hardware o software che implementa protocolli di sola lettura a livello BIOS/driver, bloccando comandi ATA/SCSI di modifica.

Hardware:

- Tableau TX1 T8u
- UltraBlock USB 3.0
- Logicube Falcon-NEO

Software (!!!):

- SafeBlock
- PDBlock

🖥️ Strumenti di Analisi

- EnCase Forensic
  Analisi file system, ricerca per parole chiave, timeline
- FTK Imager Pro
  Indicizzazione veloce, analisi email, recupero password
- Autopsy / The Sleuth Kit
  Open source, moduli Python estendibili
- X-Ways Forensics
  Supporto RAID

📡 Strumenti di Cattura Live

- Belkasoft RAM Capturer
  Bypass anti-debugging in kernel mode
- FTK Imager
  Cattura veloce e intuitiva
- DumpIt
  Massima flessibilità e opzioni
- Volatility
  Open source, Architettura a plugin per estrazione di informazioni


Tableau
Tableau
Drive Power 2
SATA/SAS 2
SATA/SAS 1
Drive Power 1


Tableau Forensic USB 3.0 Bridge
Digital Intelligence
Powered by TABLEAU
Tableau
QUICK REFERENCE GUIDE
GETTING STARTED

Strategie di acquisizione

⚡ Live Acquisition

- Sistema acceso e funzionante
- Strumenti forensi eseguiti direttamente sul sistema da acquisire
- Preserva informazioni critiche temporanee
- Fondamentale per malware memory-resident e Full Disk Encryption (BitLocker, FileVault, VeraCrypt).

💤 Static Acquisition

- Sistema spento (offline)
- Immagine bit-a-bit del disco
- Garantisce integrità del file system
- Cattura dati memorizzati (e, in qualche caso, cancellati)
- Più semplice da gestire e documentare

Memorie persistenti: aspetti critici

Hard Disk Drive (HDD)

Velocità: 2–8 GB/min

- Analisi S.M.A.R.T. e spazio non allocato
- Verifica HPA tramite comando ATA "IDENTIFY DEVICE"
- Analisi DCO (Device Configuration Overlay)
- Settori di servizio e bad sector mapping

Solid State Drive (SSD)

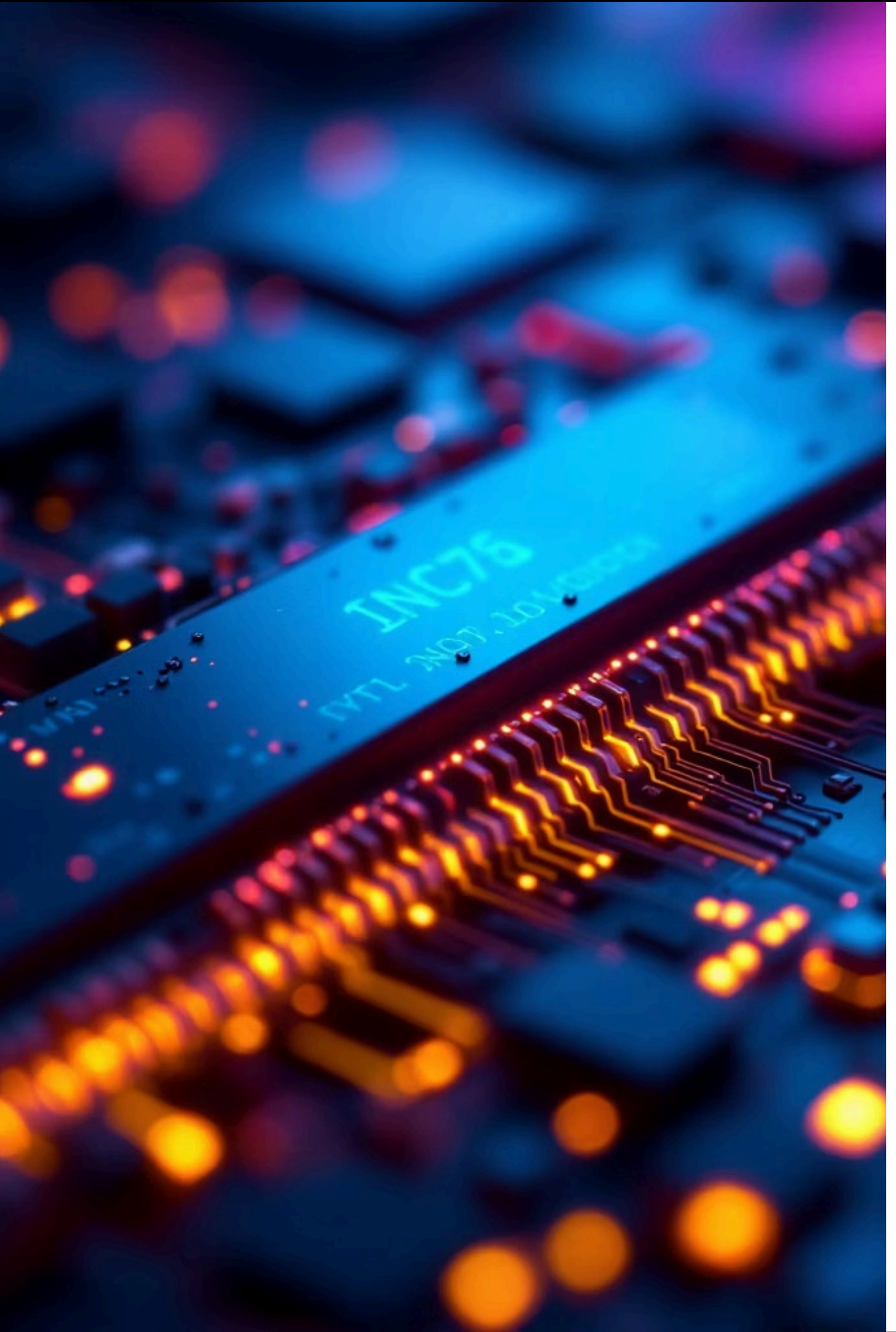
Velocità: 8–20 GB/min

- Garbage collection, TRIM e wear leveling proprietari
- Algoritmi SandForce, IntelliProp
- Write-blocker hardware NON proteggono da TRIM
- Accorgimenti per prevenire secure erase

Supporti Rimovibili (USB, SD)

Velocità: ~900 MB/min (variabile)

- Firmware controller: Phison, SMI, JMicron
- Partizioni di servizio nascoste
- eMMC integrate: BOOT1/BOOT2/RPMB



Memorie non persistenti: aspetti critici

Credenziali e Password

Password e contenuti di volumi cifrati (TrueCrypt, BitLocker, PGP Disk), credenziali per webmail e social network (Gmail, Facebook, Twitter)

Token e Chiavi

Token per servizi di file sharing (Dropbox, OneDrive), chiavi di cifratura e token di sessione attivi

Processi Attivi

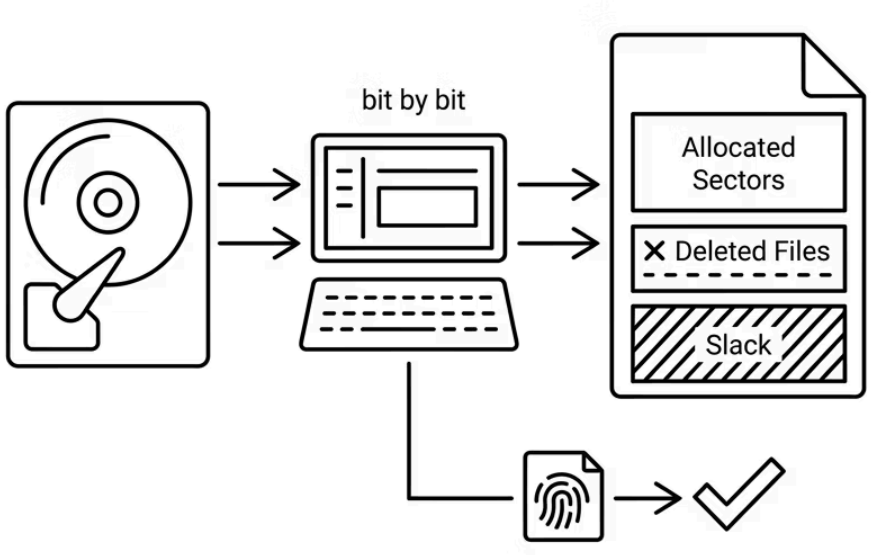
Processi con PID, PPID, nome eseguibile e timestamp. Connessioni TCP/UDP con indirizzi, porte e stato

Codice Malware

Codice iniettato da malware in processi legittimi, visibile solo in memoria e non su disco

Fonti: Belkasoft RAM Capturer, Varonis — Memory Forensics for Incident Response

Static acquisition: approcci



Copia Bit-a-Bit (Disk Imaging)

Duplicazione dell'intero supporto inclusi settori allocati, non allocati, file cancellati e spazio slack.

Formati immagine:

- DD (Raw)
- EO1 (EnCase)
- AFF4

Verifica integrità: MD5, SHA-1, SHA-256

Acquisizione Logica

Estrazione selettiva dei soli file visibili e delle strutture del file system, preservando metadati come timestamp, permessi e attributi estesi.

File system supportati:

- FAT, NTFS (Windows)
- EXT4 (Linux)
- APFS (macOS/iOS)

Protocolli: MTP/AFC per dispositivi mobili, API OAuth per cloud storage

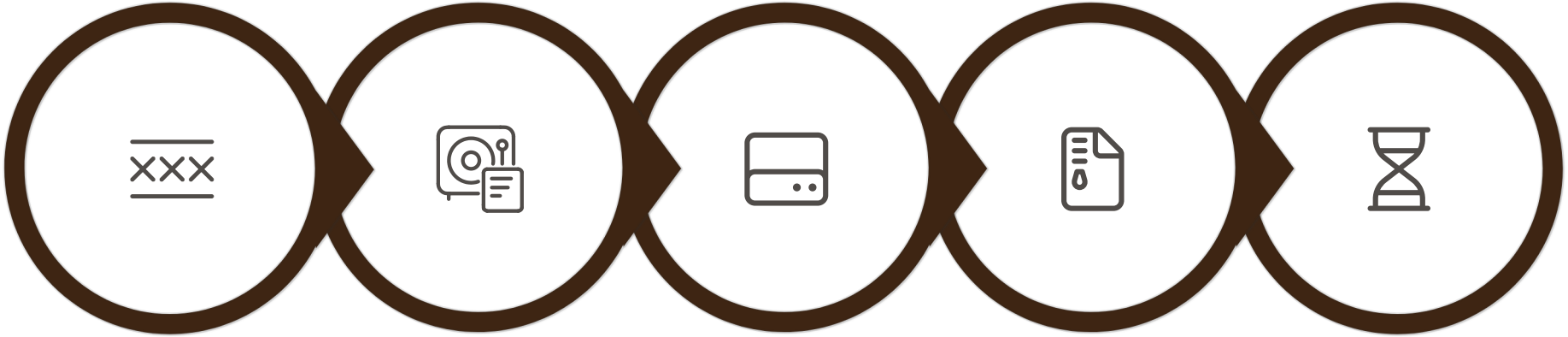
Acquisizione "Full File System"

Copia **completa** del file system entrando nel merito del contenuto del dispositivo.

Artifact recuperabili:

Lista delle applcazioni, eventi del filesystem, cronologia ricerche, uso della rete

Creazione di un'Immagine di memoria persistente con FTK Imager



Collega write blocker!

Seleziona sorgente

Scegli formato archiviazione

Inserisci informazioni sul caso

Attendi l'estrazione...

FTK Imager è uno strumento gratuito che crea copie di memorie persistenti alterare l'originale. Include funzione integrata di integrity checking con report automatico di MD5, SHA1 e bad sector.
*Fonti: **TOJO P. Thomas (Medium)***

Confronto formati di acquisizione memorie persistenti

Test effettuato su immagini DVR. *Fonte:* ***Magnet Forensics***

Formato	Caratteristiche	Performance	Note
RAW (DD)	Copia grezza, nessuna compressione, nessun metadato aggiuntivo	Ricerca 42% più veloce di E01. Imaging DVR: 1h24m, ricerca: 1h06m	Priorità alla velocità di ricerca; dati già compressi (H.264, JPEG)
E01 (EWF)	Standard forense più diffuso. Blocchi 32KB con CRC. Footer MD5. Segmenti .E01/.E02...	Imaging DVR: 1h27m, ricerca: ~1h53m. Compressione lossless fino al 50%	Formato più utilizzato; dati non compressi; compatibilità massima

Conclusioni: Per drive DVR con dati già compressi (H.264, JPEG), il formato **DD è preferibile** per performance di analisi. E01 rimane lo standard per la maggior parte delle indagini.

Hash e Verifica d'Integrità

Cos'è un hash: un'impronta digitale calcolata dal contenuto di un file o disco. Anche un solo bit modificato cambia completamente l'hash.

128 bit — MD5

Algoritmo più veloce, vulnerabile a collisioni.

Se proprio lo si vuole usare, sempre in combinazione con altri.

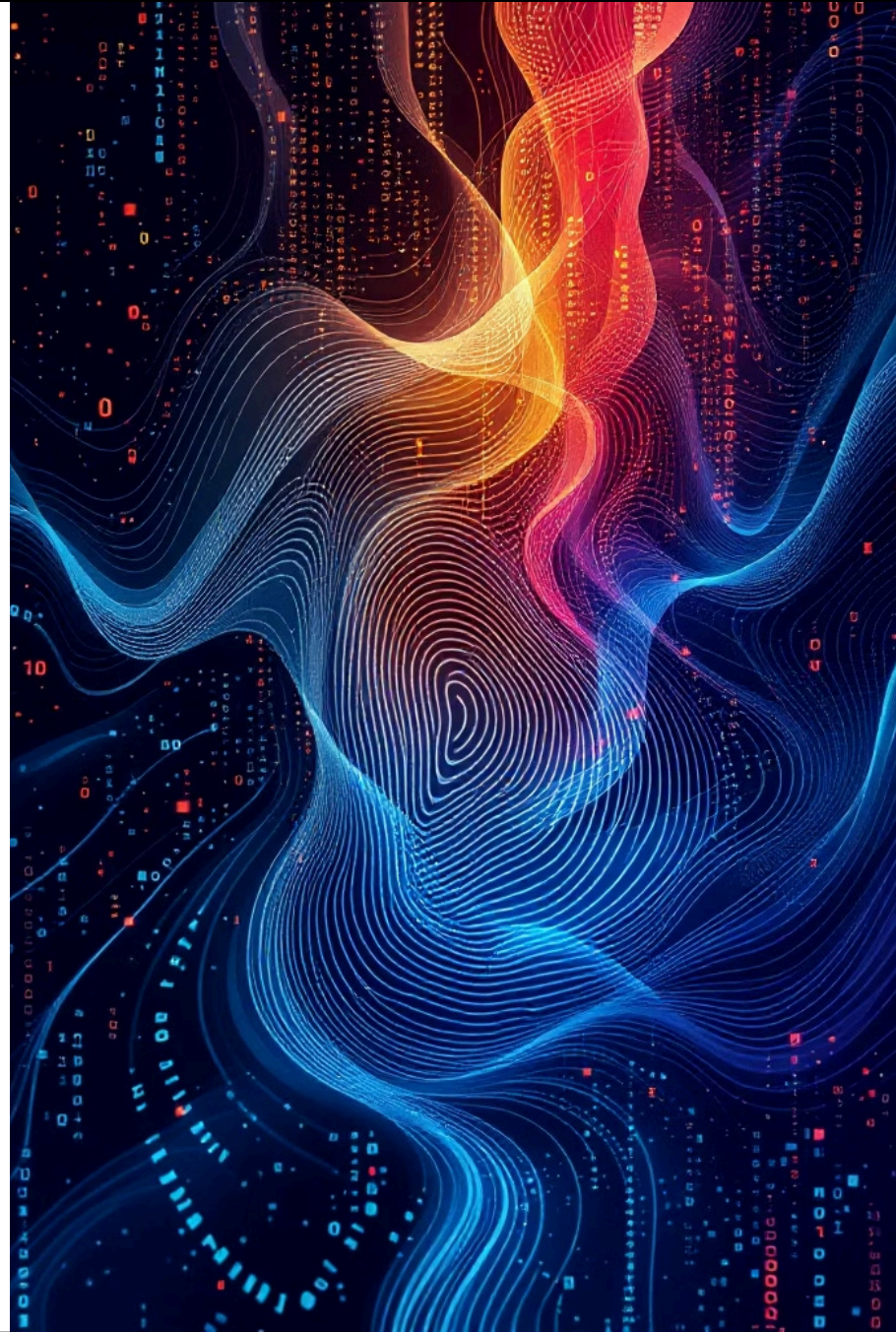
160 bit — SHA-1

Maggiore sicurezza rispetto a MD5. Ancora diffuso in ambito forense.

256 bit — SHA-256

Standard attuale più sicuro. Raccomandato per tutte le nuove acquisizioni forensi.

L'hash garantisce l'**integrità delle prove digitali**. Se l'hash rimane identico tra l'originale e la copia, l'immagine non è stata alterata. Più lungo l'hash, maggiore la sicurezza crittografica.



Criticità del calcolo hash nelle acquisizioni forensi *live*

Dump RAM

Il calcolo hash ha poco senso per dimostrare la corrispondenza con i dati originali (la memoria cambia continuamente). Resta necessario per garantire che il dump non venga modificato dopo l'acquisizione.

Computer accesi

Per imaging di computer accesi, gli hash saranno naturalmente diversi tra acquisizioni consecutive a causa dei dati volatili in continua evoluzione.

Best practice: Calcolare hash dell'intera sorgente dati E di tutti i file contenuti prima di qualsiasi analisi. Utilizzare almeno due algoritmi (es. MD5 + SHA256).
Fonte: ***MCSI Library — "Hashing for Data Integrity"***

Analisi di primo livello delle memorie persistenti

→ Esame delle strutture visibili

Analisi approfondita di NTFS, FAT32, EXT4, APFS con navigazione completa delle strutture allocate

→ Recupero File Cancellati

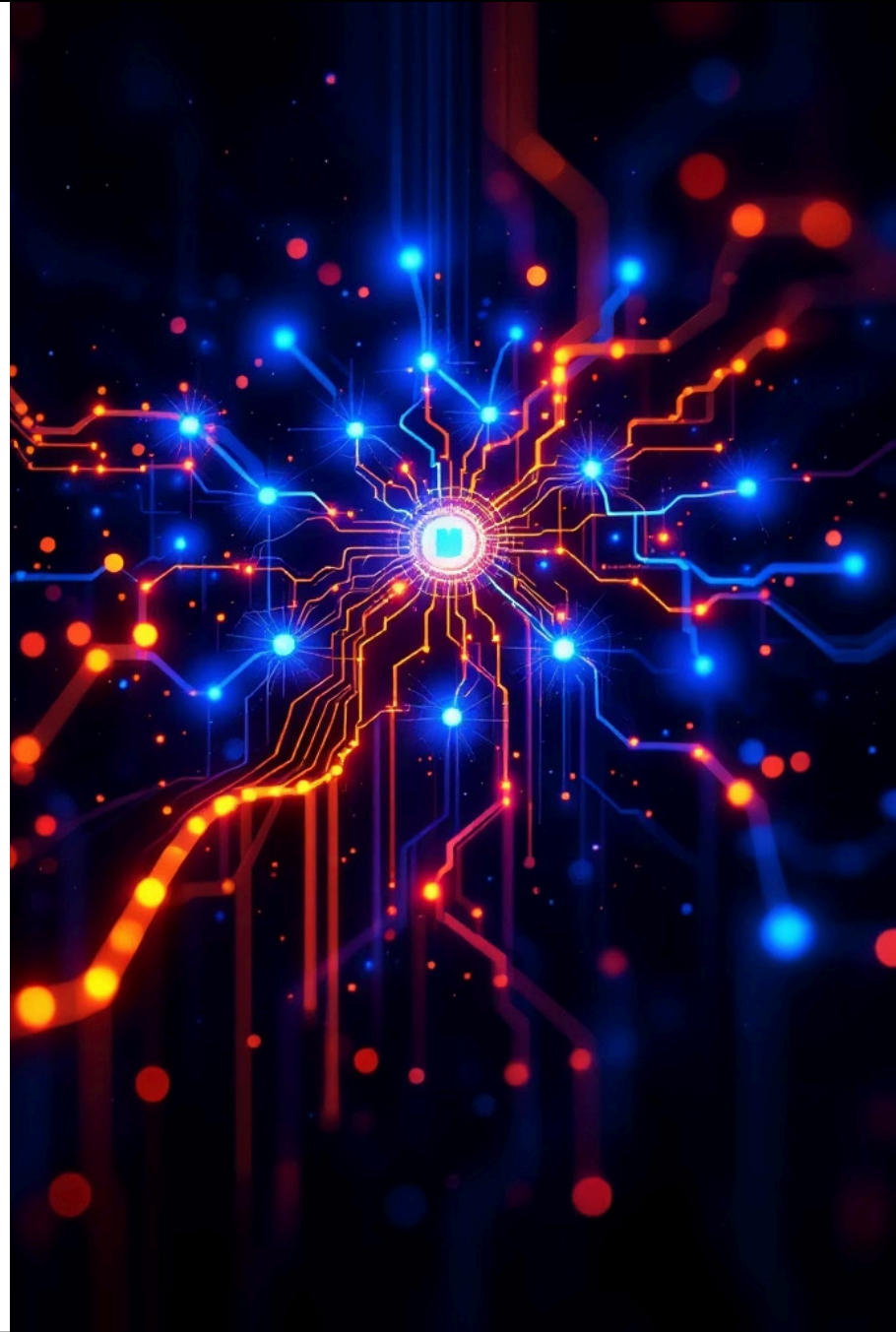
Tecniche di **carving** sequenziale e basato su firme (file magic) per recuperare dati eliminati

→ Analisi Timeline MACB

Estrazione dettagliata dei timestamp Modified-Accessed-Created-Birth e metadati EXIF/IPTC

→ Verifica Firme File

Corrispondenza tra estensioni dichiarate e signatures effettive per identificare tecniche di offuscamento



Analisi con Autopsy: Timeline e Ricostruzione Eventi

Autopsy permette di ricostruire la sequenza temporale degli eventi attraverso il modulo Timeline, estraendo tutti i timestamp e ordinandoli cronologicamente.

1. Creazione File

Registra quando un file è stato creato nel sistema

2. Modifica Contenuto

Indica quando il contenuto è stato alterato

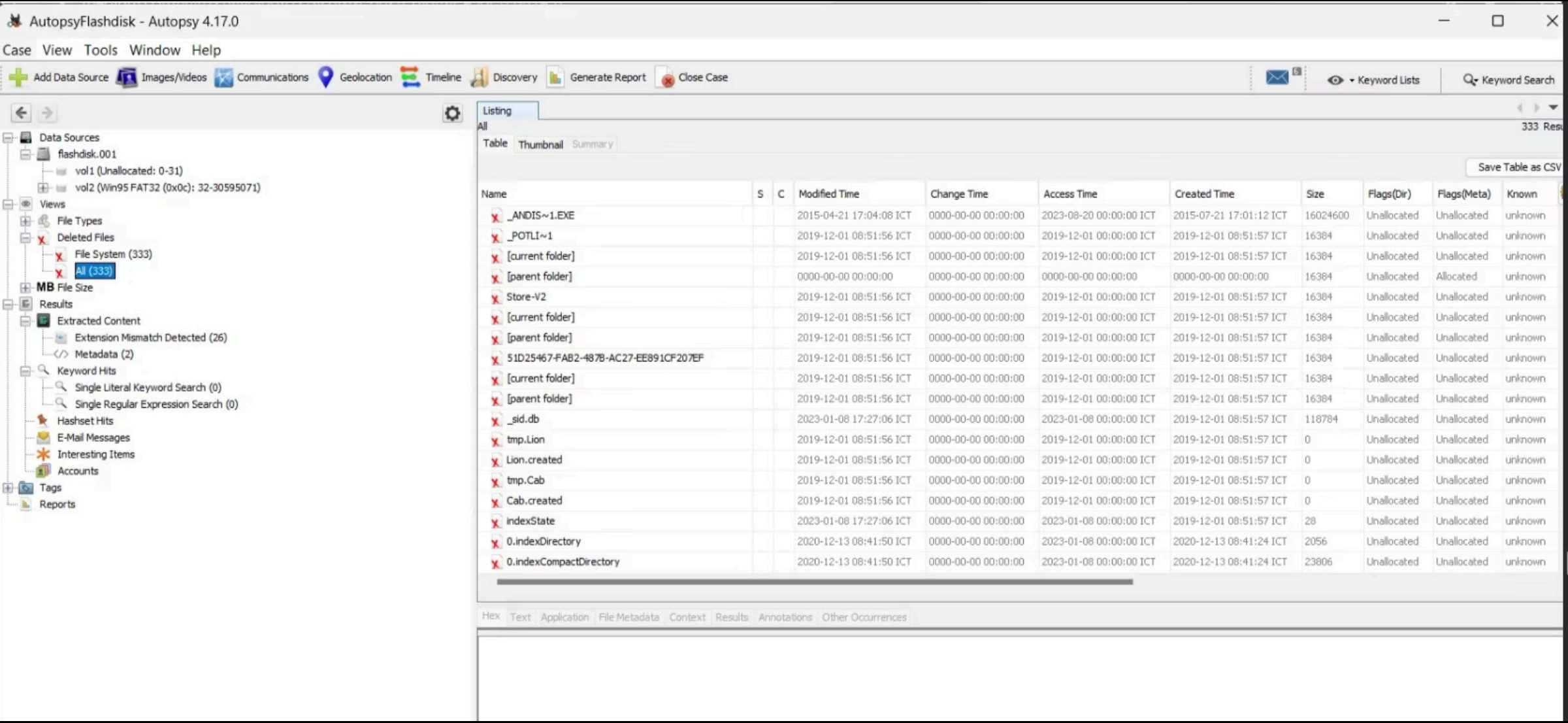
3. Ultimo Accesso

Segnala quando il file è stato aperto o letto, rivelando pattern di utilizzo

4. Modifica Metadati

Registra cambiamenti nei permessi o attributi, spesso correlati a tentativi di nascondere informazioni

Esempio pratico: dispositivo contenente fil creato il 3 maggio alle 10:15, modificato alle 10:17, con modifica delle impostazioni di sistema due minuti dopo. Autopsy Metadata Analysis visualizza strutture inode (FFS/EXT), MFT entries (NTFS), directory entries (FAT), calcola MD5 e confronta con hash database noti. ***Fonte: Yogasatriuama - Medium***


AutopsyFlashdisk - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
flashdisk.001
vol1 (Unallocated: 0-31)
vol2 (Win95 FAT32 (0x0c): 32-30595071)
Views
File Types
Deleted Files
File System (333)
All (333)
File Size
Results
Extracted Content
Extension Mismatch Detected (26)
Metadata (2)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
All
333 Resu
Table Thumbnail Summary
Save Table as CSV
Name S C Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known
_ANDIS~1.EXE 2015-04-21 17:04:08 ICT 0000-00-00 00:00:00 2023-08-20 00:00:00 ICT 2015-07-21 17:01:12 ICT 16024600 Unallocated Unallocated unknown
_POTLI~1 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
[current folder] 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
[parent folder] 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 16384 Unallocated Allocated unknown
Store-V2 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
[current folder] 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
[parent folder] 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
51D25467-FAB2-487B-AC27-EE891CF207EF 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
[current folder] 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
[parent folder] 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 16384 Unallocated Unallocated unknown
_sid.db 2023-01-08 17:27:06 ICT 0000-00-00 00:00:00 2023-01-08 00:00:00 ICT 2019-12-01 08:51:57 ICT 118784 Unallocated Unallocated unknown
tmp.Lion 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 0 Unallocated Unallocated unknown
Lion.created 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 0 Unallocated Unallocated unknown
tmp.Cab 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 0 Unallocated Unallocated unknown
Cab.created 2019-12-01 08:51:56 ICT 0000-00-00 00:00:00 2019-12-01 00:00:00 ICT 2019-12-01 08:51:57 ICT 0 Unallocated Unallocated unknown
indexState 2023-01-08 17:27:06 ICT 0000-00-00 00:00:00 2023-01-08 00:00:00 ICT 2019-12-01 08:51:57 ICT 28 Unallocated Unallocated unknown
0.indexDirectory 2020-12-13 08:41:50 ICT 0000-00-00 00:00:00 2023-01-08 00:00:00 ICT 2020-12-13 08:41:24 ICT 2056 Unallocated Unallocated unknown
0.indexCompactDirectory 2020-12-13 08:41:50 ICT 0000-00-00 00:00:00 2023-01-08 00:00:00 ICT 2020-12-13 08:41:24 ICT 23806 Unallocated Unallocated unknown
Hex Text Application File Metadata Context Results Annotations Other Occurrences

MAC Times: Il Fondamento dell'Analisi Temporale

I MAC times sono metadati del file system che registrano quando determinati eventi sono avvenuti.

M — Modification Time (mtime)

Quando il **contenuto del file** è stato modificato l'ultima volta. Il file system non confronta i dati scritti con quelli esistenti: anche sovrascrivere con dati identici aggiorna il timestamp.

A — Access Time (atime)

Quando il file è stato **aperto per la lettura** l'ultima volta. Da Windows Vista in poi, l'aggiornamento dell'access time è **disabilitato di default** per motivi di performance.

C — Change/Creation Time (ctime)

Interpretato diversamente tra Unix e Windows. **Unix:** ultima modifica dei metadati (permessi, proprietario). **Windows:** data di creazione del file ("birth time"). Questa differenza può portare a presentazioni errate dei timestamp.

NTFS memorizza sia l'orario di creazione e di modifica del file. Alcuni programmi per evitare perdite di dati scrivono su un nuovo file e lo rinominano, perdendo i metadati originali (mitigato dal **File System Tunneling** di Windows).
Fonte: ***Wikipedia — MAC times***

Analisi di secondo livello delle memorie persistenti

Spazio Non Allocato

Esame specialistico con scan sequenziali e pattern-matching per recuperare dati residui non visibili al file system

File Slack Analysis

Analisi dei file slack per frammenti di dati residui tra la fine logica e la fine fisica del cluster

Partizioni Nascoste

Rilevamento tramite analisi MBR/GPT e discrepanze nei settori. Identificazione di volumi cifrati

Steganografia

Tecniche avanzate per contenuti steganografici (LSB insertion, DCT, wavelet) in file multimediali

Password Cracking

Dictionary attack, rainbow tables e brute force con accelerazione GPU per recupero credenziali

Memory Forensics con Volatility 3

Framework per l'analisi della memoria non persistente. Supporta Windows, Unix e snapshot di macchine virtuali (.vmem). Non richiede configurazione manuale del profilo OS (miglioramento rispetto alla versione 2).

Funzioni principali

Processi (windows.pslist)

Tabella processi attivi con PID, PPID, nome eseguibile e timestamp. Identifica processi anomali.

Connessioni di rete (windows.netscan)

Connessioni TCP/UDP con indirizzi, porte e stato. Identifica comunicazioni sospette.

Code injection (windows.malfind)

Rilevamento codice iniettato in processi legittimi. Analizza regioni di memoria per malware.

Dati Sensibili Recuperabili

Chiavi di Cifratura

Chiavi attive in memoria, illeggibili su disco

Token e Password

Credenziali presenti in memoria durante la sessione

VM Snapshot

File .vmem analizzabile direttamente con Volatility

Fonti: ***Varonis — "How to Use Volatility for Memory Forensics and Analysis"***, ***Varonis — "Memory Forensics for Incident Response"***

Confronto Strumenti di Acquisizione RAM

Tempi di acquisizione di 16 GB di RAM. *Fonte:* ***Thanursan, Medium***

Tool	Sviluppatore	Tempo	Note
FTK Imager	AccessData	59 sec ⚡	GUI, opzione cattura pagefile inclusa
RAM Capture**r**	Belkasoft	61 sec	GUI, gratuito, **funziona con protezioni anti-debug**
RAM Capture	Magnet Forensics	85 sec	GUI, interfaccia intuitiva
DumpIt	Comae Toolkit/Magnet Forensics	133 sec	CLI, maggior varietà di opzioni ma più lento

Conclusione: Tutti i tool con GUI hanno superato DumpIt in velocità. FTK Imager offre anche l'opzione di catturare il pagefile per un'analisi più completa.

Scrivere la relazione/1

Prima di Iniziare

- Nomina del consulente tecnico (art. 359 c.p.p.) o del perito (art. 221 c.p.p.)
- Definizione dell'incarico e dei quesiti tecnici
- Indicazione specifica dei supporti da acquisire

Contenuto della Relazione

- Identificazione supporti: seriale, marca, modello, capacità
- Documentazione fotografica e codice univoco
- Catena di custodia: data, ora, operatore, motivo per ogni accesso
- Verbale di consegna per ogni trasferimento
- Log operazioni con timestamp certificato
- Software utilizzati (versione e configurazione)
- Write-blocker impiegati
- Modalità di acquisizione selezionata
- Report hash: supporto originale E copia forense

Scrivere la relazione/2

1 Metodologie Documentate

Documentazione minuziosa delle metodologie utilizzate con indicazione di software, versioni e parametri applicati

2 Catalogazione Cronologica

Risultati ottenuti con riferimenti temporali UTC e catalogazione cronologica verificabile

3 Limitazioni Tecniche

Esplicitazione delle limitazioni tecniche dell'analisi e del grado di confidenza nei risultati

Il report dello strumento di acquisizione e analisi, da solo, non è sufficiente. Il report deve descrivere chiaramente come la catena di custodia è stata mantenuta durante l'intero caso.

L'esaminatore deve complementare le funzioni di reporting del prodotto con informazioni su:

- strumenti aggiuntivi utilizzati;
- sorgenti dati e modalità di acquisizione;
- come ne è stata garantita l'integrità e come sono stati esaminati e analizzati.
  *Fonte: **Belkasoft — "Preserving chain of custody in digital forensics**"*

Grazie per l'attenzione!