CORSO AVANZATO DI DIGITAL FORENSICS

Acquisizione forense da personal computer e server

File cancellati, timeline e navigazione Internet: dall’immagine del disco alla ricostruzione dei fatti

Relatore: Vincenzo Calabrò

Materiale didattico con fonti normative e scientifiche aggiornate a novembre 2026.

Programma e obiettivi della mezza giornata

Parte	Contenuto	Durata
1	Il computer come fonte di prova	25 min
2	Quadro normativo e standard	35 min
	Pausa	15 min
3	Metodo: immagine, memoria, file cancellati, date, navigazione	60 min
4	Laboratorio guidato con strumenti open source	70 min
5	Caso di studio, quiz di verifica, bibliografia	35 min

Quattro ore complessive. In laboratorio si lavora su un'immagine disco sintetica costruita per il corso, mai su dati reali.

Al termine lo studente è in grado di

- scegliere fra acquisizione a macchina spenta, live e selettiva, e motivare la scelta a verbale;
- recuperare un file cancellato per tre vie diverse e dire che cosa restituisce ciascuna;
- costruire una timeline dal file system e leggerne le date senza forzarle;
- ricostruire la navigazione dai database del browser e riportarla sulla stessa timeline.

PARTE 1 · 25 MINUTI

Il computer come fonte di prova

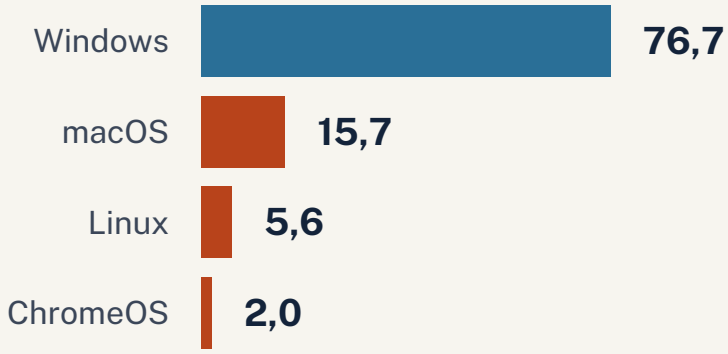
Un disco conserva più di quanto mostra: file che l’utente crede cancellati, date che nessuno ha scritto di proposito, pagine visitate. Cifratura e SSD stanno riducendo questo margine.

Di quali computer parliamo

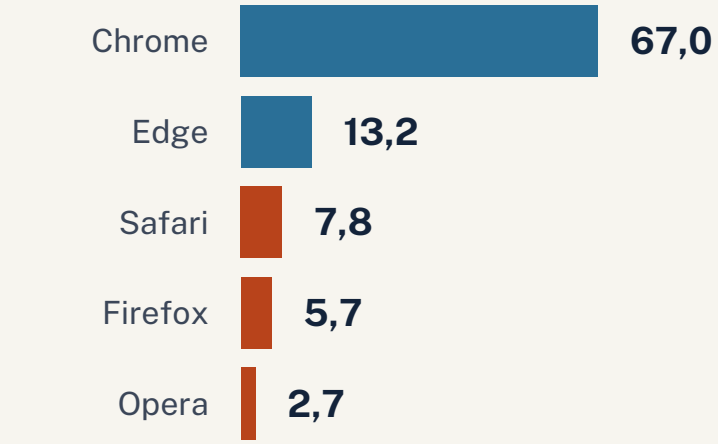
74 %

dei computer Windows in uso a ottobre 2026 ha Windows 11; il 25 % è rimasto a Windows 10.

Sistemi operativi desktop, quota in %



Browser su desktop, quota in %



Tre computer su quattro usano NTFS e quattro navigazioni su cinque passano da un browser Chromium, cioè Chrome o Edge, che condividono il formato. Il laboratorio parte da qui.

Fonte: StatCounter Global Stats, mondo, ottobre 2026. La voce macOS somma «OS X» e «macOS» della fonte. Le barre scure indicano ciò che si esamina in laboratorio.

Dove stanno le evidenze

Si perde allo spegnimento

Memoria volatile

Processi, connessioni di rete, chiavi di cifratura, schede del browser ancora aperte.

Disco

File system

File presenti con nomi e date; record dei file cancellati che il sistema non ha ancora riusato.

Disco

Spazio non allocato

Contenuto di file cancellati che non hanno più un nome. Su SSD con TRIM dura poco.

Disco

Registri e log

Registry, Event Log, journal del file system; sui server, log dei servizi e delle autenticazioni.

Disco

Profili utente

Documenti, collegamenti recenti, database del browser, client di posta e di sincronizzazione.

Disco e altrove

Copie e versioni

Cestino, shadow copy, snapshot, backup, versioni nel cloud: lo stesso file in un altro momento.

I file cancellati si cercano nel secondo, nel terzo e nel sesto riquadro. La timeline li attraversa tutti; la navigazione sta nel quinto e, in parte, nel primo.

L’ordine di volatilità

N.	Che cosa	Quanto dura
1	Registri e cache del processore	Nanosecondi
2	Tabelle di routing, cache ARP, tabella dei processi, memoria	Fino allo spegnimento
3	File system temporanei	Fino al riavvio
4	Disco	Fino alla sovrascrittura
5	Log remoti e dati di monitoraggio	Secondo la politica di conservazione
6	Configurazione fisica e topologia di rete	Finché l’impianto non cambia
7	Supporti di archivio	Anni

Si acquisisce dall’alto verso il basso. Su un server acceso, cominciare dal disco significa rinunciare alle prime tre righe.

Fonte: Brezinski D., Killalea T., RFC 3227, 2002, par. 2.1 per l’ordine; la colonna «Quanto dura» è una sintesi didattica.

Le quattro domande del quesito

File

Che cosa c’era

Quali file esistevano, quali sono stati cancellati e se il loro contenuto si può ancora recuperare.

Timeline

Quando

In che ordine sono avvenute creazione, modifica, copia e cancellazione, e con quale margine d’errore.

Navigazione

Che cosa è stato cercato

Ricerche, pagine, download e caricamenti; che cosa ne resta se la cronologia è stata svuotata.

Attribuzione

Chi

Quale account era in sessione. Dall’account alla persona si arriva per inferenza, con altri elementi.

Il quesito si scrive prima dell’acquisizione. Delimita che cosa cercare e in quale arco di tempo: è ciò che permette di selezionare i dati pertinenti e di restituire il resto.

Le prime tre risposte stanno nel disco. La quarta non si trova in nessun file: si argomenta.

Quattro modi di acquisire

	File cancellati	Timeline	Navigazione	Memoria volatile
Post-mortem, immagine completa	**Sì**	**Sì**	**Sì**	No
Live, a sistema acceso	In parte	**Sì**	**Sì**	**Sì**
Selettiva, per artefatti	No	In parte	**Sì**	In parte
Remota, con agent	No	In parte	**Sì**	In parte

- **Post-mortem**: «Sì» vale per un disco leggibile. Con un volume cifrato e senza chiave la riga diventa tutta «No».
- **Live**: è l'unica via alla memoria e, su un volume cifrato già aperto, ai dati in chiaro. Altera il sistema: ogni comando va a verbale.
- **Selettiva e remota**: raccolgono artefatti scelti, non lo spazio non allocato. Bastano per navigazione e log, non per il carving.

Valutazione qualitativa proposta per la discussione in aula; non deriva da una misurazione.

PARTE 2 · 35 MINUTI

Quadro normativo e standard

Dal 2008 il codice chiede che la copia sia conforme e immodificabile. Dal 2025 la Cassazione chiede anche di dire prima che cosa si cerca, in quale periodo, e quando si restituisce il resto.

Venticinque anni di norme, standard e tecnologia

2001
Convenzione di Budapest sulla criminalità informatica

2002
RFC 3227: ordine di volatilità e raccolta delle prove

2006
NIST SP 800-86: tecniche forensi nella risposta agli incidenti

2008
L. 48/2008: copia conforme e immodificabile nel c.p.p.

2012
ISO/IEC 27037 su identificazione, raccolta e acquisizione

2015
ISO/IEC 27041, 27042 e 27043 su metodi, analisi e processo

2017
Cass., Sez. Un., n. 40963: sulla copia trattenuta resta l'interesse al riesame

2023
SWGDE 17-F-002 v2.0 sulle acquisizioni da computer; Reg. (UE) 2023/1543

2024
Windows 11 24H2 estende la cifratura automatica del disco; il Senato approva il ddl sull'art. 254-ter

2025
Cass. n. 17479 e n. 34324: oggetto e periodo nel decreto; fine del supporto a Windows 10

2026
e-Evidence applicabile dal 18 agosto

In corso
Disegno di legge sull'art. 254-ter c.p.p., all'esame della Camera

Gli standard tecnici sono fermi al 2012–2015. Da allora sono cambiati i dischi e sono cresciute le garanzie: il metodo deve tenere conto di entrambe le cose.

Italia: che cosa chiede il codice a chi opera

Istituto	Norma del c.p.p.	Che cosa chiede
Ispezione informatica	art. 244, co. 2	Misure tecniche che conservino i dati originali e ne impediscano l'alterazione
Perquisizione informatica	art. 247, co. 1-bis	Le stesse cautele, anche se il sistema è protetto da misure di sicurezza
Sequestro di dati presso fornitori	art. 254-bis	Copia su adeguato supporto, con procedura che ne assicuri conformità e immodificabilità
Custodia	art. 260, co. 2	Copia dei dati su adeguati supporti, conforme all'originale e non modificabile
Urgenza della polizia giudiziaria	artt. 352, co. 1-bis, e 354, co. 2	Dove possibile, duplicazione immediata su adeguati supporti
Accertamenti tecnici	artt. 359 e 360	Se l'operazione non è ripetibile, avviso alle parti, che possono assistere con propri consulenti

Il codice non prescrive uno strumento né un formato: prescrive un risultato. Spetta a chi opera dimostrare, con hash e verbale, di averlo ottenuto.

Fonte: codice di procedura penale, come modificato dalla L. 18 marzo 2008, n. 48.

Sequestro, copia integrale e proporzionalità

Dottrina e giurisprudenza

Copia-mezzo e copia-fine

La copia integrale serve a selezionare. Finita la selezione, ciò che non è pertinente si restituisce, copia compresa. Il codice non usa questi termini.

Cass., sez. II, n. 34324/2025; sez. VI, n. 17479/2025

Oggetto e periodo nel decreto

Quali informazioni si cercano, in quale arco di tempo ed entro quando avverrà la selezione: sono indicazioni del decreto, non della fase di estrazione.

Cass., Sez. Un., n. 40963/2017; sez. VI, n. 40677/2025

Restituire il dispositivo non basta

Finché l'autorità trattiene la copia dei dati, l'interessato conserva l'interesse a chiedere il riesame del sequestro.

Cass., sez. III, n. 41055/2025

Una copia tracciabile

La selezione segue i criteri fissati dall'autorità e opera su una copia integrale che resta tracciabile e immodificabile.

Per il tecnico: filtri per periodo e parole chiave a verbale, elenco dell'estratto, restituzione documentata del resto. Il disegno di legge sull'art. 254-ter c.p.p., approvato dal Senato il 10 aprile 2024, a settembre 2026 era ancora all'esame della Camera.

I riferimenti giurisprudenziali vanno riscontrati sulle banche dati ufficiali prima di essere citati in un atto.

Oltre il codice: cooperazione, dati personali, azienda

Quando il server è altrove

Cooperazione

Convenzione di Budapest, artt. 19 e 29–32: perquisizione e sequestro di dati, conservazione rapida, assistenza fra Stati.

Reg. (UE) 2023/1543: ordini europei di produzione e di conservazione rivolti ai prestatori di servizi, applicabile dal 18 agosto 2026.

Sempre

Protezione dei dati

Dir. (UE) 2016/680 e d.lgs. 51/2018 per le autorità; Reg. (UE) 2016/679 per tutti gli altri.

Minimizzazione e limitazione della conservazione valgono anche per la copia forense e per le copie di lavoro.

Indagine interna

Il computer aziendale

Art. 4 L. 300/1970 sui controlli a distanza; Linee guida del Garante su posta elettronica e Internet, 2007; Corte EDU, Bărbulescu c. Romania, 2017.

Informazione preventiva, finalità determinata, proporzionalità: la proprietà del computer non basta a renderlo ispezionabile.

Lo scenario del laboratorio è un'indagine interna. Prima del primo comando servono un incarico scritto, una policy nota al dipendente e un perimetro.

Gli standard tecnici di riferimento

Documento	Edizione	Che cosa copre
ISO/IEC 27037	2012, confermata nel 2018	Identificazione, raccolta, acquisizione e conservazione
ISO/IEC 27041, 27042, 27043	2015	Idoneità dei metodi, analisi e interpretazione, processo d'indagine
NIST SP 800-86	2006	Tecniche forensi nella risposta agli incidenti
RFC 3227	2002	Ordine di volatilità, errori da evitare, catena di custodia
SWGDE 17-F-002	v2.0, 2023	Acquisizioni da computer: fisica, logica, mirata, live
SWGDE 18-F-001	v2.0	Esame dei supporti dopo l'acquisizione
NIST CFTT	programma in corso	Prove su imaging, write blocker, recupero di file cancellati, carving

Nessuno di questi documenti è una norma di legge. Seguirli, e dichiarare dove ci si è discostati, è ciò che rende difendibile il metodo.

Dal requisito all’artefatto

Requisito	Che cosa lo soddisfa
Identità del supporto	Marca, modello, numero di serie, capacità, fotografie; per un server, anche lo schema dei volumi e del RAID
Integrità della copia	Hash dell’immagine calcolato all’acquisizione e riverificato a ogni apertura; write blocker o avvio forense
Completezza	Immagine dell’intero supporto, spazio non allocato compreso; se selettiva, elenco di ciò che resta fuori e perché
Ripetibilità	Strumenti e versioni a verbale, comandi salvati in file, risultati chiave ottenuti con due strumenti
Collocazione nel tempo	Fuso e scarto dell’orologio annotati; ogni data riportata in UTC insieme alla sua fonte
Proporzionalità	Filtri per periodo e parole chiave dichiarati; restituzione documentata dei dati non pertinenti
Attribuzione	Account, profilo e sessione tenuti distinti dalla persona; riscontri esterni al computer

Ogni riga senza artefatto è una domanda già pronta per il controesame.

PARTE 3 · 60 MINUTI

Metodo: dall’immagine alla ricostruzione

Prima si decide come acquisire, memoria compresa. Poi si cerca ciò che è stato cancellato, si mettono in ordine le date e si legge la navigazione. Ogni passaggio ha un limite fisico che va dichiarato.

Acceso o spento: la prima decisione

Se è acceso: non spegnere subito

1. Fotografare lo schermo e annotare l’ora reale e quella mostrata dal sistema.
2. Verificare se il volume è cifrato e aperto: da spento potrebbe non riaprirsi.
3. Acquisire la memoria, poi i dati volatili, poi il disco.
4. Soltanto dopo decidere se spegnere, e in che modo.

Se è spento: non accendere

1. Non avviare il sistema installato: ogni avvio riscrive file e date.
2. Estrarre il disco e collegarlo a un write blocker, oppure avviare da un supporto forense.
3. Acquisire l’intero supporto e calcolarne l’hash.
4. Se il volume è cifrato, cercare la chiave di ripristino presso il titolare, l’amministratore o l’account.

Windows 11 24H2 attiva la cifratura del disco durante l’installazione, quando si accede con un account Microsoft. Spegnere un portatile recente può chiudere una porta che non si riapre.

Fonti: SWGDE 17-F-002 v2.0, 2023; SWGDE, Best Practices for Digital Evidence Collection; per Windows 11 24H2, dichiarazioni di Microsoft riportate dalla stampa tecnica nel 2024.

L’immagine forense

Formato	Caratteristiche
raw (dd)	Copia settore per settore, senza metadati; la leggono tutti gli strumenti
E01	Expert Witness: compressione, hash e dati del caso dentro il file
AFF4	Contenitore aperto, adatto anche a immagini logiche e di memoria

In sola lettura. Write blocker hardware, oppure avvio da una distribuzione forense come CAINE o Tsurugi Linux, che non monta i dischi in scrittura.

Settori illeggibili. Si annotano nel log dell’acquisizione; non si saltano in silenzio.

DALLA DOCUMENTAZIONE: NON ESEGUITI NEL CORSO

```
$ dc3dd if=/dev/sdb of=caso.dd \
    hash=sha256 log=caso.log
copia raw, hash calcolato in lettura
$ ewfacquire /dev/sdb
copia E01; chiede i dati del caso
$ ewfverify caso.E01
ricalcola l’hash e lo confronta
```

L’immagine copia tutto il supporto, spazio non allocato compreso. Una copia dei soli file visibili non contiene ciò che è stato cancellato.

Fonti: documentazione di dc3dd e di libewf; NIST CFTT, Disk Imaging.

Memoria volatile: perché viene prima

Stato del sistema

Che cosa stava accadendo

Processi in esecuzione, con riga di comando e ora di avvio; moduli caricati; connessioni di rete aperte; utenti in sessione.

Dati in chiaro

Ciò che il disco cifra

Chiavi dei volumi cifrati aperti, documenti non salvati, contenuto delle schede del browser, anche in navigazione privata.

Solo in memoria

Ciò che il disco non vede

Codice caricato senza passare da un file, comandi digitati in una shell, testo copiato negli appunti.

Tre casi in cui decide l'esito. Un portatile con il disco cifrato e aperto. Un server compromesso, dove l'intruso lavora in memoria. Una navigazione privata, o una cronologia appena svuotata.

È l'unica fonte che lo spegnimento distrugge per intero. Per questo si acquisisce prima del disco, e l'operazione non è ripetibile.

Fonti: RFC 3227; SWGDE 17-F-002 v2.0; Ligh M. H. et al., The Art of Memory Forensics, Wiley, 2014; Case A., Richard G. G., Memory forensics: The path forward, Digital Investigation, 2017.

Acquisire la memoria

Scenario	Fonte o strumento	Attenzione
Windows acceso	WinPmem, open source	Windows 11 può rifiutarne il driver
Linux acceso	AVML, oppure il modulo LiME	Il kernel in lockdown limita l'accesso
Macchina virtuale	Snapshot o sospensione dall'hypervisor	Nessuna traccia nel sistema ospite
Da remoto	Velociraptor	Dump in rete: canale cifrato e hash
Spento o ibernato	hiberfil.sys, pagefile.sys, swap, crash dump	Memoria precedente, già sul disco
macOS	Sui Mac recenti è di fatto preclusa	Raccolta live di processi e log

Lo strumento gira sul sistema in esame: si avvia da un supporto esterno, scrive su un supporto esterno, e ogni passo va a verbale con la sua ora.

Fonti: documentazione di WinPmem (Velocidex), AVML (Microsoft), LiME e Velociraptor; Volatility 3, documentazione 2.28, che non mantiene più il supporto a macOS.

Analizzare con Volatility 3

Domanda	Plugin
Che sistema è?	windows.info, banners
Che cosa era in esecuzione?	windows.pslist, pstree, psscan, cmdline
Con chi comunicava?	windows.netscan, netstat
Che cosa aveva caricato o aperto?	windows.dlllist, handles, filescan
C'è codice iniettato?	windows.malfind
E su Linux?	linux.pslist, bash, lsmod, sockstat

DALLA DOCUMENTAZIONE: NON ESEGUITI NEL CORSO

```
$ vol -f memoria.raw windows.info
$ vol -f memoria.raw windows.pstree
$ vol -f memoria.raw windows.netscan
$ vol -f memoria.raw windows.cmdline --pid 4321
```

Due elenchi. pslist segue la lista dei processi tenuta dal sistema; psscan cerca le loro strutture in tutta la memoria e trova anche quelli terminati o nascosti. La differenza fra i due è già un risultato.

Dal maggio 2025 Volatility 3 ha sostituito Volatility 2, ora archiviato. Non usa più i profili: ricava le strutture da tabelle di simboli, che per Linux vanno generate per il kernel esatto.

Fonti: Volatility Foundation, annuncio del 16 maggio 2025 e documentazione 2.28. Nomi dei plugin verificati su Volatility 3 2.28.2, installato da PyPI il 29 novembre 2026.

Che cosa aggiunge la memoria alle tre domande

File cancellati

Ancora aperti

Un file cancellato dal disco può essere ancora aperto o mappato da un processo: windows.filescan lo elenca, windows.dumpfiles ne estrae le pagine presenti. E con la chiave del volume, se è in memoria, torna leggibile l’immagine di un disco cifrato.

Timeline

Gli ultimi minuti

Ogni processo porta la sua ora di avvio, ogni connessione quella di apertura. Il plugin timeliner raccoglie le date di tutti gli altri e le scrive nel formato body: si accodano alla timeline del disco, come al passo 9 del laboratorio.

Navigazione

Anche se privata

Indirizzi, titoli e contenuto delle pagine restano nei processi del browser. windows.memmap estrae la memoria di un processo; strings e bulk_extractor vi cercano URL, indirizzi di posta, termini del quesito.

La memoria non sostituisce il disco: lo completa negli ultimi minuti prima dell’intervento, che spesso sono quelli che interessano.

Fonti: Volatility 3, documentazione 2.28; Ligh et al., 2014; Garfinkel S., Digital media triage with bulk data analysis and bulk_extractor, Computers & Security, 2013.

Una prova: la navigazione privata in memoria

```
studente@vm:~/memoria$ PID=$(pgrep -o -f profilo-privato)
studente@vm:~/memoria$ python3 pmdump.py $PID > privata.mem
studente@vm:~/memoria$ strings -a privata.mem | grep -c ALFA-7731
67
studente@vm:~/memoria$ strings -a privata.mem | grep -m 1 riservato.html
http://127.0.0.1:8765/riservato.html?codice=ALFA-7731
studente@vm:~/memoria$ strings -a privata.mem | grep -m 1 "7731 - Google"
Pagina di prova ALFA-7731 - Google Chrome for Testing (Incognito)
studente@vm:~/memoria$ pkill -o -f profilo-privato
studente@vm:~/memoria$ sqlite3 -readonly profilo-privato/Default/History "SELECT count(*) FROM visits"
0
studente@vm:~/memoria$ sqlite3 -readonly profilo-normale/Default/History "SELECT count(*) FROM visits"
1
studente@vm:~/memoria$
```

Che cosa si è fatto. Un browser Chromium in modalità Incognito apre una pagina di prova su un server locale. A sessione aperta, uno script di venti righe copia la memoria scrivibile del processo: 340 MB.

Che cosa risulta. L'indirizzo compare 67 volte, con il titolo della finestra che dichiara la modalità. Chiuso il browser, la cronologia contiene zero visite; la stessa pagina, in una sessione normale, ne lascia una.

Che cosa non è. È la memoria di un processo, non un'immagine della RAM. Su un'immagine completa lo stesso risultato si cerca con Volatility e windows.memmap.

Schermata originale del 29 novembre 2026: Chrome for Testing 153 su Linux, pagina e codice di prova. Lo script è nel pacchetto del docente.

Memoria: limiti e cautele

Acquisizione

Immagine non atomica

La memoria cambia mentre viene copiata. Ne escono strutture incoerenti e plugin che falliscono; più RAM, più incoerenza.

Acquisizione

Non tutto è in RAM

Pagine compresse o spostate su pagefile e swap: si acquisiscono insieme al dump, altrimenti mancano pezzi.

Analisi

Stringhe senza contesto

Un indirizzo trovato con strings non ha data né autore. Come un file da carving, dice che c'era, non quando.

Garanzie

Dati di terzi

In memoria ci sono password e contenuti estranei al quesito. Valgono proporzionalità e selezione, come per la copia del disco.

A verbale. Ora di inizio e di fine, strumento e versione, supporto di destinazione, hash del dump, motivo per cui si è scelto di non spegnere.

Un dump imperfetto resta utile, purché l'imperfezione sia dichiarata. Un dump non fatto non si recupera.

Fonti: Vömel S., Freiling F., Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition, Digital Investigation, 2012; Pagani F., Fedorov O., Balzarotti D., Introducing the Temporal Dimension to Memory Forensics, ACM TOPS, 2019.

Dal personal computer al server

Aspetto	Personal computer	Server
Disponibilità	Si può spegnere e portare via	Spesso deve restare in servizio
Supporti	Un disco, di solito SSD	RAID, volumi logici, storage di rete
Forma	Macchina fisica	Spesso virtuale: disco, snapshot e memoria sono file dell'hypervisor
Evidenze tipiche	Profilo utente, documenti, browser	Log dei servizi, autenticazioni, database, job pianificati
Volume	Centinaia di gigabyte	Terabyte: l'acquisizione selettiva diventa la regola
Interlocutore	L'utilizzatore	L'amministratore, che può essere a sua volta un interessato

Di un RAID si acquisisce il volume logico e, quando si può, anche i singoli dischi. Di una macchina virtuale si chiede all'hypervisor uno snapshot che comprenda la memoria.

Che cosa succede quando si cancella un file

Dove	Che cosa fa la cancellazione	Che cosa resta
Cestino	Sposta il file in $Recycle.Bin e ne descrive l'origine in un file $I	Tutto: nome, percorso, data di cancellazione, contenuto
NTFS	Segna libero il record nella $MFT e i cluster nella $Bitmap; toglie la voce dalla cartella	Nome, date e posizione dei dati, finché il record non viene riusato
FAT, exFAT	Marca libera la voce di directory e libera i cluster	Nome, date e primo cluster
ext4	Azzera gli extent nell'inode e vi scrive la data di cancellazione	Il nome nella directory; la posizione dei dati soltanto nel journal
APFS	Rimuove i record del file; i blocchi non vengono riscritti sul posto	Versioni precedenti negli snapshot

La cancellazione ordinaria non sovrascrive il contenuto. Stabilisce soltanto per quanto tempo il file system ricorda dove si trova.

Fonti: Carrier B., File System Forensic Analysis, 2005; Fairbanks K., An analysis of Ext4 for digital forensics, DFRWS 2012; Hansen K. H., Toolan F., Decoding the APFS file system, Digital Investigation, 2017.

Tre livelli di recupero

Livello	Da dove	Che cosa restituisce	Limite
1. Copie logiche	Cestino, shadow copy, snapshot, backup, versioni nel cloud	Nome, percorso, date e contenuto	Esistono soltanto se l'utente o il sistema le hanno create
2. Metadati del file system	Record della $MFT o inode non ancora riusati	Nome, date e, se i cluster sono intatti, il contenuto	Il record viene riusato dal primo file creato dopo
3. Carving	Firme di formato nello spazio non allocato	Il solo contenuto	Niente nome né date; file frammentati incompleti; falsi positivi

Come riferirlo. Un file recuperato dal livello 2 «esisteva con questo nome e queste date». Uno recuperato dal livello 3 «era presente sul supporto»: quando e con quale nome va cercato altrove.

Si procede dall'alto. Ogni livello restituisce meno del precedente e chiede più cautela nel riferirlo.

Fonti: Carrier, 2005; Garfinkel S., Carving contiguous and fragmented files with fast object validation, Digital Investigation, 2007; Pal A., Memon N., The evolution of file carving, IEEE Signal Processing Magazine, 2009.

SSD, TRIM e cifratura: i limiti fisici

	Record del file	Contenuto dai metadati	Carving
Disco magnetico	**Sì**	**Sì**	**Sì**
SSD interno, TRIM attivo	**Sì**	No	No
SSD senza TRIM, supporti USB	**Sì**	In parte	In parte
Volume cifrato, senza chiave	No	No	No

- **TRIM.** Alla cancellazione il sistema comunica all'SSD i blocchi liberati; il controller li ripulisce per conto proprio, anche dietro un write blocker.
- **La misura.** King e Vidas hanno provato sedici unità: con TRIM la pulizia può avvenire in pochi secondi.
- **Che cosa resta comunque.** Il record nella $MFT, i file piccoli residenti nel record, il Cestino, i journal, le copie su altri supporti.

Fonti: King C., Vidas T., Empirical analysis of solid state disk data retention, DFRWS 2011; Bell G., Boddington R., JDFSL, 2010. La matrice è una sintesi qualitativa.

Otto date per ogni file

	Data	Cambia quando
M	Modified	cambia il contenuto
A	Accessed	il file viene letto, se l'aggiornamento è attivo
C	Changed	cambia il record: nome, attributi, dimensione
B	Born	il file nasce su quel volume

In NTFS le quattro date esistono due volte: in $STANDARD_INFORMATION, che è ciò che mostra il sistema, e in $FILE_NAME, che si aggiorna a creazione, rinomina e spostamento.

Regole di lettura

- Una copia nasce oggi ma conserva la data di modifica dell'originale: M anteriore a B indica un file copiato o scaricato.
- Le date di $STANDARD_INFORMATION si possono riscrivere. Se B vi precede quella di $FILE_NAME c'è un indizio di alterazione, non una prova.
- Da Windows 10 1803 la data di accesso è gestita dal sistema: si aggiorna se il volume di sistema non supera 128 GB.
- NTFS registra in UTC con passo di 100 nanosecondi; FAT in ora locale, con passo di due secondi.

Prima di ordinare le date se ne annotano tre cose: fuso orario del sistema, scarto del suo orologio, stato dell'aggiornamento della data di accesso.

Fonti: Carrier, 2005; Chow K. P. et al., The Rules of Time on NTFS File System, SADFE 2007; documentazione Microsoft su NtfsDisableLastAccessUpdate.

Windows: gli artefatti che datano un’azione

Artefatto	Che cosa data	Attenzione
$UsnJrnl:$J	Creazione, rinomina e cancellazione di ogni file	Ha dimensione fissa: copre giorni o settimane
Event Log	Accessi, avvii, servizi, dispositivi	Si può svuotare; l’evento 1102 lo registra
Prefetch	Esecuzione di un programma, con le ultime volte	Di norma disattivato su Windows Server
LNK e Jump List	Apertura di un file, anche su supporti poi rimossi	Dicono che è stato aperto, non da chi
ShellBags	Cartelle esplorate, anche se poi cancellate	Solo ciò che passa da Esplora risorse
SRUM	Uso della rete e delle risorse per applicazione	Dati aggregati, per circa un mese
Registry, USBSTOR	Supporti USB collegati, prima e ultima volta	Da incrociare con setupapi.dev.log

Sui Copilot+ PC dove l’utente ha attivato Recall c’è una fonte in più: istantanee dello schermo e testo riconosciuto, in un database SQLite cifrato dentro il profilo.

Fonti: SANS, Windows Forensic Analysis; Kaspersky Securelist, 2026, sugli artefatti di Windows 11; documentazione Microsoft su Recall. Durate indicative, variabili con versione e configurazione.

Linux e macOS: server e portatili

Linux, soprattutto server

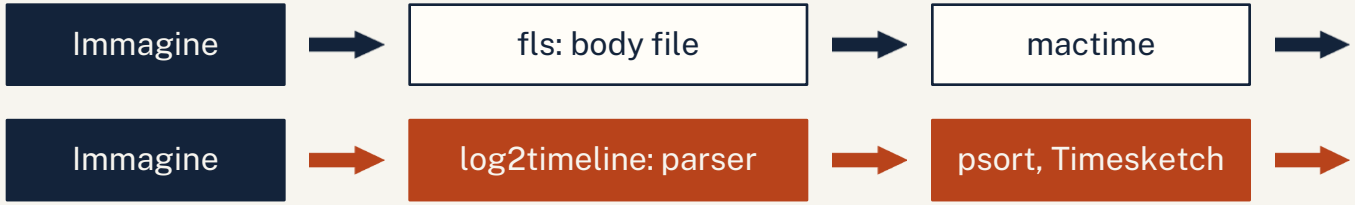
- **journald e /var/log**: servizi, kernel, autenticazioni
- **wtmp, btmp, lastlog**: sessioni, tentativi falliti, ultimo accesso
- **.bash_history**: comandi, senza orario se non è configurato
- **cron, timer, log dei pacchetti**: che cosa è stato pianificato e installato
- **auditd**, se attivo: chi ha eseguito che cosa
- **ext4**: data di creazione e di cancellazione nell'inode

macOS

- **Unified Log**: attività di sistema e applicazioni, per un tempo limitato
- **FSEvents**: creazioni, modifiche e cancellazioni per volume
- **KnowledgeC e Biome**: uso delle applicazioni
- **QuarantineEvents**: file scaricati, con l'URL di origine
- **Snapshot APFS e Time Machine**: versioni precedenti dei file

Su un server i log sono l'evidenza principale e il primo bersaglio di chi vuole coprire le tracce. La copia inviata a un sistema esterno vale più di quella locale.

Dalla timeline del file system alla super timeline



Timeline del file system. Quando è cambiato ciascun file.

Super timeline. Anche ciò che i file contengono: log, Registry, visite del browser.

PLASO, DALLA DOCUMENTAZIONE: NON ESEGUITO NEL CORSO

```
$ log2timeline.py --storage-file caso.plaso caso.dd
$ psort.py --output_time_zone UTC -o dynamic -w super.csv caso.plaso
```

Come si legge. Si parte da un punto fermo, per esempio l'ora di un download, e si allarga la finestra di qualche minuto alla volta. Leggere milioni di righe dall'inizio non porta a nulla.

In laboratorio la fusione si fa a mano, con mactime e sqlite3: lo stesso principio, in venti righe.

Fonti: Guðjónsson K., Mastering the Super Timeline with log2timeline, SANS, 2010; Hargreaves C., Patterson J., An automated timeline reconstruction approach for digital forensic investigations, Digital Investigation, 2012.

Navigazione: dove sono i dati

Browser	Database della cronologia	Formato e date
Chrome	`%LocalAppData%\Google\Chrome\User Data\Default\History`	SQLite. Microsecondi dal 1° gennaio 1601, UTC
Edge	`%LocalAppData%\Microsoft\Edge\User Data\Default\History`	Come Chrome: stesso motore, stesso schema
Firefox	`%AppData%\Mozilla\Firefox\Profiles\<profilo>\places.sqlite`	SQLite. Microsecondi dal 1° gennaio 1970, UTC
Safari	`~/Library/Safari/History.db`	SQLite. Secondi dal 1° gennaio 2001, UTC

Attenzione. Chrome recente tiene il database in modalità WAL: insieme a History si copiano History-wal e History-shm, altrimenti le ultime visite restano fuori.

Tre epoche per lo stesso istante. Scambiarle sposta una visita di 369 anni o di 31, e l’errore si vede. Quello di fuso orario è di un’ora o due, e non si vede.

Fonti: codice sorgente di Chromium; documentazione Mozilla; percorsi predefiniti, variabili con profilo e versione. Modalità WAL verificata su Chrome for Testing 153.

Navigazione: che cosa si ricava

Fonte	Che cosa contiene	Che cosa prova
urls, visits	URL, titolo, ora di ogni visita, provenienza, tipo di transizione	Che la pagina è stata caricata in quel profilo, e come ci si è arrivati
keyword_search_terms	Il testo delle ricerche	L'intenzione, più di qualunque URL
downloads	URL di origine, percorso di salvataggio, inizio, fine, byte	Il legame fra una pagina e un file sul disco
Cache	Copie di pagine, immagini, script	Che cosa mostrava la pagina
Cookies, Login Data	Sessioni e credenziali, cifrate con chiavi del sistema	L'uso di un account su un sito
Sessions	Schede aperte all'ultima chiusura	Che cosa era aperto in quel momento

Il tipo di transizione distingue un indirizzo digitato da un link seguito o da un reindirizzamento: separa la visita voluta da quella subita.

Fonti: Oh J., Lee S., Lee S., Advanced evidence collection and analysis of web browser activity, Digital Investigation, 2011; codice sorgente di Chromium. Nomi delle tabelle riferiti ai browser Chromium.

Navigazione cancellata, privata, sincronizzata

Cronologia svuotata

Può restare qualcosa

SQLite non sempre azzera le righe eliminate: possono sopravvivere nelle celle libere, nei file -wal e -journal, nelle shadow copy. Dipende dal browser e dalla versione, e il recupero va validato.

Navigazione privata

Fuori dal browser

Non scrive nel database della cronologia. Le tracce stanno altrove: memoria, file di paging e di ibernazione, cache DNS, esecuzione del programma, volumi di traffico.

Profilo sincronizzato

Visite fatte altrove

Con un account sincronizzato compaiono pagine visitate su un altro dispositivo. In Chromium la tabella visit_source ne indica l'origine: si controlla prima di attribuirle al computer in esame.

L'assenza di cronologia non prova l'assenza di navigazione. Una cronologia presente prova l'uso di un profilo, non l'identità di chi sedeva alla tastiera.

Fonti: Aggarwal G. et al., An analysis of private browsing modes in modern browsers, USENIX Security 2010; Ohana D. J., Shashidhar N., Do private and portable web browsers leave incriminating evidence?, 2013; Pawlaszczyk D., Hummert C., Making the invisible visible, 2021.

Strumenti open source, fase per fase

Fase	Strumenti	Nota
Acquisizione	dc3dd, ewfacquire, Guymager; CAINE, Tsurugi	Avvio forense o write blocker
Memoria	AVML, LiME, WinPmem; Volatility 3, MemProcFS	Operazione non ripetibile
File cancellati	The Sleuth Kit, Autopsy	Stessa libreria: a riga di comando o con interfaccia grafica
Carving	PhotoRec, foremost, scalpel, bulk_extractor	Su una copia dello spazio non allocato
Timeline	mactime, plaso, Timesketch	Fuso orario dichiarato in ogni esportazione
Artefatti Windows	RegRipper, strumenti di Eric Zimmerman	Verificare le versioni di Windows coperte
Navigazione	sqlite3, Hindsight	Su copie dei database, mai sugli originali
Raccolta selettiva	Velociraptor, UAC, DFIR-ORC	Elenco degli artefatti raccolti a verbale

Open source non significa validato: per i risultati che contano, due strumenti diversi e un solo esito.

Versioni correnti a novembre 2026: The Sleuth Kit 4.14.0 (aprile 2025), Autopsy 4.23.0 (aprile 2026), dai siti dei progetti.

PARTE 4 · 70 MINUTI

Laboratorio guidato

Un’immagine disco di 65 MB, un collaboratore in uscita, venti minuti di un pomeriggio di novembre. Undici passi con The Sleuth Kit, foremost e sqlite3.

Scenario e regole del laboratorio

Scenario

Uno studio tecnico sospetta che un collaboratore, prima di lasciare l'incarico il 20 novembre 2026, abbia portato fuori l'elenco dei clienti e il listino riservato. Il portatile aziendale è stato acquisito a macchina spenta, su incarico scritto e nel perimetro della policy interna.

Quesito. Dire se i due file sono stati copiati o trasmessi, quando, e che cosa è stato cancellato.

Cartella di lavoro: caso05. Contiene caso05.dd, immagine raw con una partizione NTFS, e tre file .sql con le query.

Regole

L'immagine è sintetica: volume creato con ntfs-3g, date impostate per lo scenario, nomi e siti di fantasia sotto il dominio .example.

Si lavora sull'immagine in sola lettura. Ogni file estratto va in una cartella a parte, con il suo hash.

Ogni comando finisce a verbale con data e ora in UTC, compresi quelli sbagliati.

Undici passi: i primi cinque cercano i file, i tre successivi il tempo e la navigazione, gli ultimi tre compongono il quadro.

Passo 1: verificare l’immagine e orientarsi

ESEGUITO IN LABORATORIO, OUTPUT ABBREVIATO

```
$ sha256sum caso05.dd
8792793e3cfa6df36ddbecb57900755c77314f1d8f092a95642773f1bba5f18d  caso05.dd
$ mmls caso05.dd
      Slot      Start        End          Length       Description
002:  000:000   0000002048   0000133119   0000131072   NTFS / exFAT (0x07)
$ fsstat -o 2048 caso05.dd
File System Type: NTFS    Volume Name: DATI    Cluster Size: 4096
```

Hash. Si confronta con quello del verbale di acquisizione prima di ogni altra operazione, e di nuovo alla fine.

Partizioni. Una sola, dal settore 2048: è il valore dell’opzione -o in tutti i comandi che seguono.

File system. NTFS con cluster da 4.096 byte. Il nome del volume e il numero di serie vanno a verbale.

Comandi eseguiti il 28 novembre 2026 con The Sleuth Kit 4.12.1 su Ubuntu 24.04. L’output di fsstat è riportato su una riga.

Passo 2: ciò che ha ancora un record

```
studente@vm:~/caso05$ fls -o 2048 -rpd caso05.dd | grep -v Orphan
-/r * 90-128-2: Users/collab/Documents/export/clienti_2026.zip
studente@vm:~/caso05$ icat -o 2048 caso05.dd 90 > recuperati/clienti_2026.zip
studente@vm:~/caso05$ unzip -l recuperati/clienti_2026.zip
Archive:  recuperati/clienti_2026.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
     3295  2026-11-12 10:14   elenco_clienti.csv
     3863  2026-10-21 12:05   listino_riservato.csv
---------                     -------
     7158                     2 files
studente@vm:~/caso05$ sha256sum recuperati/clienti_2026.zip
fa1ed8e8a67c2f50173b9a1f612c8e9f90edc47ece1b4ca989936997881cddf7  recuperati/clienti_2026.zip
studente@vm:~/caso05$
```

Elencare. fls con -d mostra i soli record cancellati: ne risulta uno, clienti_2026.zip, record 90. Le voci «OrphanFile» escluse dal filtro sono record riservati e mai usati di un volume appena creato.

Recuperare. icat legge il contenuto seguendo il record, anche se il file non è più allocato. L’archivio si apre e contiene proprio i due file del quesito. Gli orari interni allo ZIP sono in ora locale.

Schermata originale, prodotta il 28 novembre 2026 sull’immagine sintetica caso05.dd.

Passo 3: leggere il record

```
ESEGUITO IN LABORATORIO, OUTPUT ABBREVIATO
$ istat -o 2048 -z UTC caso05.dd 90
Entry: 90        Sequence: 2
Not Allocated File
$STANDARD_INFORMATION Attribute Values:
Created:        2026-11-19 16:48:02.001371000 (UTC)
$FILE_NAME Attribute Values:
Name: clienti_2026.zip
Parent MFT Entry: 89    Sequence: 1
Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 1840  init_size: 1840
2213
```

Stato. Il record è libero, ma nome, date e posizione dei dati sono ancora leggibili: nessun file creato dopo lo ha riusato.

Origine. Creato alle 16:48:02 UTC del 19 novembre nella cartella con record 89, cioè Documents\export.

Contenuto. 1.840 byte nel cluster 2213. Finché nessuno lo riscrive, il file si recupera intero.

Comando eseguito il 28 novembre 2026 sull’immagine sintetica; sono riportate dieci righe dell’output.

Passo 4: il Cestino

```
ESEGUITO IN LABORATORIO, OUTPUT ABBREVIATO
$ fls -o 2048 -p caso05.dd 79
r/r 91-128-2:   $I4K7Q2M.txt
r/r 87-128-2:   $R4K7Q2M.txt
$ icat -o 2048 caso05.dd 91 | xxd | head -n 2
00000000: 0200 0000 0000 0000 9800 0000 0000 0000  ................
00000010: 00a4 6c05 4778 dd01 2b00 0000 4300 3a00  ..l.Gx..+...C.:.
$ icat -o 2048 caso05.dd 87 | tail -n 2
- copiare elenco clienti e listino prima di venerdi
- usare il sito di trasferimento, non la posta
```

Il file $I. Dimensione originale, 152 byte, e data di cancellazione: 19 novembre 2026, 16:57:12 UTC. Segue il percorso: Desktop\note_passaggio.txt.

Il file $R. È il contenuto, intatto. Nomina i due file del quesito e il modo scelto per trasferirli.

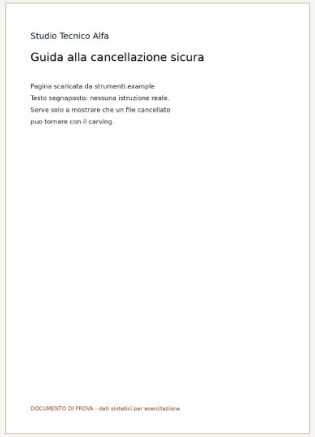
La cartella. Porta il SID dell’account: il Cestino dice anche da quale profilo è partita la cancellazione.

Comandi eseguiti il 28 novembre 2026. Nell’immagine di prova la coppia $I e $R è stata costruita a mano secondo il formato di Windows 10 e 11.

Passo 5: il file che non ha più un record

```
studente@vm:~/caso05$ blkls -o 2048 caso05.dd > nonallocato.raw
studente@vm:~/caso05$ foremost -q -t pdf,jpg -i nonallocato.raw -o carving
Processing: nonallocato.raw
|*|
studente@vm:~/caso05$ grep -A3 "^Num" carving/audit.txt
Num      Name (bs=512)         Size      File Offset     Comment

0:      00016280.pdf          71 KB         8335360
Finish: Sat Nov 28 22:48:07 2026
studente@vm:~/caso05$ pdfinfo carving/pdf/00016280.pdf | head -n 5
Title:          Guida alla cancellazione sicura
CreationDate:   Tue Sep  1 12:00:00 2026 UTC
ModDate:        Tue Sep  1 12:00:00 2026 UTC
Custom Metadata: no
Metadata Stream: no
studente@vm:~/caso05$
```


Studio Tecnico Alfa

Guida alla cancellazione sicura

Pagina scaricata da strumenti.example
Testo segnaposto: nessuna istruzione reale.
Serve solo a mostrare che un file cancellato
può tornare con il carving.

DOCUMENTO DI PROVA - dati sintetici per esercitazione

Perché serve. La cronologia registra un download, ma fls non trova il file: il suo record è stato riusato da da_fare.txt. Resta il contenuto nello spazio non allocato. blkls lo estrae, foremost vi cerca le firme dei formati.

Che cosa torna. Un PDF senza nome e senza date di file system; titolo e data interna sopravvivono. Ha 73.343 byte, uno più di quanti ne registra il browser: il contenuto è quello, l'hash no.

Schermata originale del 28 novembre 2026; a destra, la prima pagina del PDF recuperato, un documento di prova.

Passo 6: la timeline del file system

ESEGUITO IN LABORATORIO

```
$ fls -o 2048 -r -m "C:/" caso05.dd > body.txt
$ mactime -b body.txt -d -z UTC 2026-11-19..2026-11-20 > timeline.csv
$ grep 16:48:02 timeline.csv | grep -v FILE_NAME | cut -d, -f1,3,8
Thu Nov 19 2026 16:48:02,m.c.,"C:/Users/collab/Documents"
Thu Nov 19 2026 16:48:02,.a..,"C:/Users/collab/Documents/Clienti/elenco_clienti.csv"
Thu Nov 19 2026 16:48:02,.a..,"C:/Users/collab/Documents/Clienti/listino_riservato.csv"
Thu Nov 19 2026 16:48:02,.a.b,"C:/Users/collab/Documents/export"
Thu Nov 19 2026 16:48:02,macb,"C:/Users/collab/Documents/export/clienti_2026.zip (deleted)"
```

Due comandi. fls scrive una riga per ogni file, con le sue date, nel formato body; mactime le ordina e le filtra per periodo. La colonna centrale dice quali date cadono in quell’istante.

Un secondo. Alle 16:48:02 nasce l’archivio e, nello stesso istante, i due file dei clienti risultano letti. Su un sistema reale si controlla prima se la data di accesso veniva aggiornata.

Comandi eseguiti il 28 novembre 2026 sull’immagine sintetica. Gli avvisi di Perl emessi da mactime sono stati omessi.

Passo 7: la cronologia del browser

```
studente@vm:~/caso05$ sqlite3 -header -column browser/History < visite.sql
utc                 tipo  url
------------------  ----  ------------------------------------------------------------
2026-11-12 09:20:15  0     https://posta.example/inbox
2026-11-17 08:05:44  0     https://meteo.example/oggi
2026-11-18 14:22:03  5     https://ricerca.example/search?q=modello+lettera+dimissioni
2026-11-19 16:38:12  5     https://ricerca.example/search?q=inviare+file+grandi+senza+email
2026-11-19 16:39:05  0     https://trasferisci.example/
2026-11-19 16:41:30  5     https://ricerca.example/search?q=cancellare+file+definitivamente
2026-11-19 16:43:48  0     https://strumenti.example/guide/cancellazione-sicura
2026-11-19 16:50:22  0     https://trasferisci.example/upload
studente@vm:~/caso05$ sqlite3 browser/History "SELECT term FROM keyword_search_terms"
modello lettera dimissioni
inviare file grandi senza email
cancellare file definitivamente
studente@vm:~/caso05$
```

```
datetime(visit_time/1000000 - 11644473600, 'unixepoch')
```

La query. History si estrae con icat dal record 82 e se ne calcola l’hash. visite.sql unisce visits e urls e converte la data dall’epoca del 1601, con l’espressione qui sopra.

La lettura. Fra le 16:38 e le 16:50: come inviare file grandi, un sito di trasferimento, come cancellare file per sempre, una guida, la pagina di caricamento. Tipo 5 è una ricerca dalla barra degli indirizzi, 0 un link seguito.

Schermata originale del 28 novembre 2026. Il database di prova ha lo schema di Chrome ridotto alle tabelle usate; i siti sono di fantasia.

Passo 8: il download e la visita che manca

```
ESEGUITO IN LABORATORIO
$ sqlite3 -line browser/History < download.sql
     inizio = 2026-11-19 16:44:18
       fine = 2026-11-19 16:44:20
total_bytes = 73342
target_path = C:\Users\collab\Downloads\guida_cancellazione_sicura.pdf
$ sqlite3 browser/History "SELECT seq FROM sqlite_sequence WHERE name='visits'; SELECT max(id) FROM visits"
9
8
$ strings browser/History | grep k7Qm2x
https://trasferisci.example/d/k7Qm2xCaricamento completato: clienti_2026.zip
```

Il download. Lega la guida a un file che sul disco non ha più nome: stessa dimensione del PDF ricavato al passo 5, meno un byte.

La riga tolta. Nove identificativi assegnati, otto righe: una visita è stata rimossa. Il testo è ancora nel file e nomina l'archivio. È un residuo: dice che la pagina è stata vista, non quando.

Comandi eseguiti il 28 novembre 2026 sul database di prova, dove la cancellazione sicura di SQLite è disattivata.

Passo 9: una sola timeline

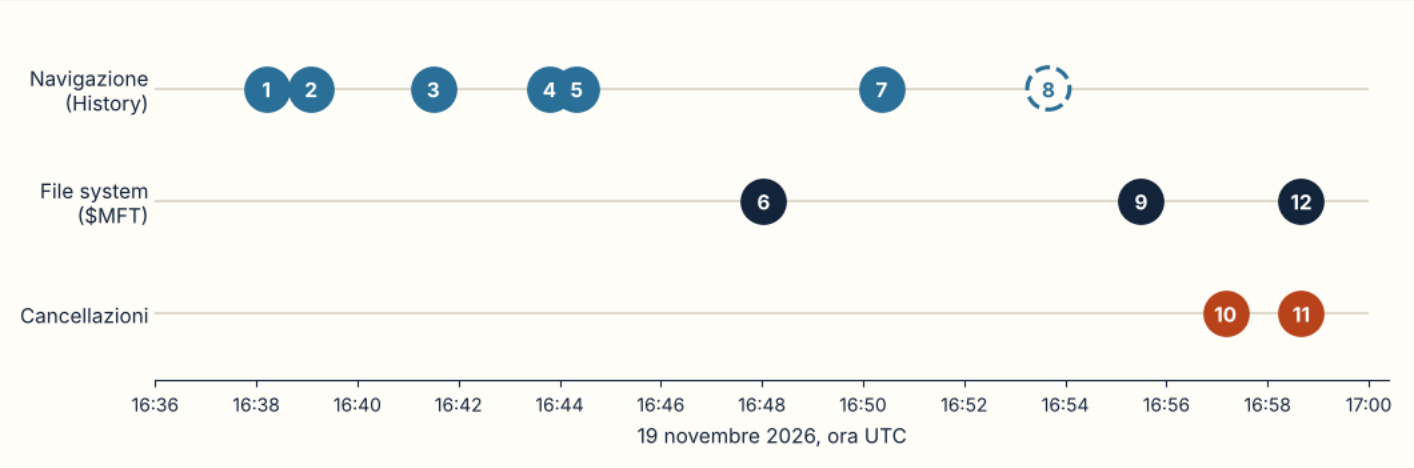
```
studente@vm:~/caso05$ cat body.txt web.body > tutto.body
studente@vm:~/caso05$ mactime -b tutto.body -d -z UTC 2026-11-19..2026-11-20 2>/dev/null | grep -v FILE_NAME | cut -d, -f1,3,8
Date,Type,File Name
Thu Nov 19 2026 16:38:12,m...,"[Chrome visita] https://ricerca.example/search?q=inviare+file+grandi+senza+email"
Thu Nov 19 2026 16:39:05,m...,"[Chrome visita] https://trasferisci.example/"
Thu Nov 19 2026 16:41:30,m...,"[Chrome visita] https://ricerca.example/search?q=cancellare+file+definitivamente"
Thu Nov 19 2026 16:43:48,m...,"[Chrome visita] https://strumenti.example/guide/cancellazione-sicura"
Thu Nov 19 2026 16:44:18,...b,"[Chrome download] C:\Users\collab\Downloads\guida_cancellazione_sicura.pdf"
Thu Nov 19 2026 16:44:20,m...,"[Chrome download] C:\Users\collab\Downloads\guida_cancellazione_sicura.pdf"
Thu Nov 19 2026 16:48:02,m.c.,"C:/Users/collab/Documents"
Thu Nov 19 2026 16:48:02,.a..,"C:/Users/collab/Documents/Clienti/elenco_clienti.csv"
Thu Nov 19 2026 16:48:02,.a..,"C:/Users/collab/Documents/Clienti/listino_riservato.csv"
Thu Nov 19 2026 16:48:02,.a.b,"C:/Users/collab/Documents/export"
Thu Nov 19 2026 16:48:02,macb,"C:/Users/collab/Documents/export/clienti_2026.zip (deleted)"
Thu Nov 19 2026 16:50:22,m...,"[Chrome visita] https://trasferisci.example/upload"
Thu Nov 19 2026 16:55:30,m.c.,"C:/Users/collab/AppData/Local/Google/Chrome/User Data/Default/History"
Thu Nov 19 2026 16:57:10,m.c.,"C:/$Recycle.Bin/S-1-5-21-1004336348-1177238915-682003330-1001"
Thu Nov 19 2026 16:57:10,..c.,"C:/$Recycle.Bin/S-1-5-21-1004336348-1177238915-682003330-1001/$R4K7Q2M.txt"
Thu Nov 19 2026 16:57:10,m.c.,"C:/Users/collab/Documents/export"
Thu Nov 19 2026 16:57:10,macb,"C:/$Recycle.Bin/S-1-5-21-1004336348-1177238915-682003330-1001/$I4K7Q2M.txt"
Thu Nov 19 2026 16:58:40,m.c.,"C:/Users/collab/Desktop"
Thu Nov 19 2026 16:58:40,m.c.,"C:/Users/collab/Downloads"
Thu Nov 19 2026 16:58:40,macb,"C:/Users/collab/Desktop/da_fare.txt"
studente@vm:~/caso05$
```

Il metodo. Una query, web.sql, scrive visite e download nel formato body. Accodate al file del passo 6, mactime le ordina insieme a tutto il resto.

La lettura. Del download delle 16:44 e del caricamento delle 16:50 il file system non sa nulla; delle cancellazioni delle 16:57 e delle 16:58 non sa nulla il browser.

Schermata originale del 28 novembre 2026 sull’immagine sintetica. Le righe $FILE_NAME sono escluse per brevità.

Passo 10: venti minuti, tre fonti



1 · 16:38 ricerca «inviare file grandi senza email»

2 · 16:39 sito di trasferimento

3 · 16:41 ricerca «cancellare file definitivamente»

4 · 16:43 guida alla cancellazione sicura

5 · 16:44 download della guida in PDF

6 · 16:48 creato l'archivio, letti i due file

7 · 16:50 pagina di caricamento

8 · conferma del caricamento: residuo senza ora

9 · 16:55 ultima scrittura di History

10 · 16:57 note nel Cestino, archivio cancellato

11 · 16:58 guida cancellata

12 · 16:58 il record della guida viene riusato

Elaborazione dai risultati dei passi 2–9, ora UTC. L'evento 8 è collocato per deduzione fra il 7 e il 9; il grafico lo mostra tratteggiato.

Passo 11: chiudere e riferire

ESEGUITO IN LABORATORIO

```
$ sha256sum recuperati/* carving/pdf/* browser/History timeline.csv > hash.txt
$ sha256sum caso05.dd
8792793e3cfa6df36ddbecb57900755c77314f1d8f092a95642773f1bba5f18d  caso05.dd
```

Si può affermare

- Un archivio con i due file è stato creato alle 16:48:02 UTC e cancellato entro le 16:57:10.
- Dal profilo sono stati visitati un sito di trasferimento, la sua pagina di caricamento e quella di conferma, che nomina l'archivio.
- Una guida alla cancellazione è stata scaricata e poi rimossa.

Non si può affermare

- Che l'archivio sia arrivato a destinazione: servono i log del servizio o della rete.
- L'ora della pagina di conferma.
- Chi fosse alla tastiera: il computer indica un profilo, non una persona.

L'hash dell'immagine, ricalcolato alla fine, coincide con quello del passo 1: l'analisi non l'ha modificata.

Otto errori ricorrenti

Accendere «per dare un’occhiata»

Ogni avvio riscrive date, log e spazio libero.

Spegnere un disco cifrato e aperto

Senza la chiave di ripristino non si riapre.

Copiare i file, non il disco

Lo spazio non allocato resta fuori, e con lui i file cancellati.

Rimandare l’acquisizione di un SSD

Il controller ripulisce da solo, anche dietro un write blocker.

Leggere le date senza fuso

Un’ora di scarto basta a spostare un alibi.

Dare nome e data a un file da carving

Non ne ha: sono inferenze, e vanno dette tali.

Aprire i database in scrittura

Il motore SQLite può modificare il file e il suo -wal.

Confondere il profilo con la persona

L’account dice chi poteva, non chi ha fatto.

La prima metà si commette prima ancora dell’analisi, e nessuno strumento la corregge dopo.

Limiti del laboratorio e liceità

Che cosa il laboratorio non mostra

- Il volume è stato scritto da ntfs-3g, non da Windows: mancano $LogFile, $UsnJrnl, Registry, Prefetch, Event Log.
- Nessuna cifratura e nessun SSD: il carving qui riesce, su un portatile recente spesso no.
- Database del browser a schema ridotto; Cestino costruito a mano; date scritte con un orologio simulato.

Fuori dall'aula

Gli stessi comandi su un computer altrui richiedono un titolo: un provvedimento dell'autorità, un incarico difensivo, oppure un incarico aziendale dentro una policy nota.

Senza titolo l'accesso a un sistema protetto è un reato, art. 615-ter c.p., anche se il metodo è impeccabile.

I dati di terzi trovati per caso non si usano e non si conservano.

Il laboratorio insegna il metodo su un caso pulito. Un caso reale aggiunge rumore, cifratura e vincoli giuridici: tutti e tre vanno dichiarati in relazione.

PARTE 5 · 35 MINUTI

Caso di studio e verifica

Dal portatile al server: lo stesso metodo, con altri vincoli. Poi otto domande per controllare che cosa è rimasto della giornata.

Caso di studio: il server che non si può fermare

Scenario

Uno studio professionale tiene gestionale e archivio documentale su un server Linux virtuale, ospitato sul proprio hypervisor. Lunedì mattina l'amministratore trova vuota la cartella dei contratti e, nei log, accessi SSH notturni da un indirizzo sconosciuto.

Per rimediare ha già riavviato la macchina e ripristinato sopra di essa il backup di venerdì.

Quesito. Che cosa è stato cancellato, quando, da quale account e da dove.

Dati e vincoli

Disco virtuale da 400 GB con file system ext4, su storage SSD.

Snapshot settimanale dell'hypervisor, la domenica alle 02:00.

Log di sistema inoltrati a un collettore esterno.

Lo studio deve tornare operativo entro la giornata.

Il caso è inventato per il corso. Le due mosse dell'amministratore sono invece quelle che si incontrano più spesso.

Caso di studio: il lavoro dei gruppi

Domanda	Che cosa consegnare
Che cosa si è perso con il riavvio e con il ripristino, e come lo si scrive a verbale?	Elenco delle fonti perse e di quelle rimaste
Che cosa si acquisisce, in quale ordine e in quale forma?	Piano di acquisizione: snapshot, disco virtuale, memoria, log esterni
Dove si cercano i file cancellati, con ext4 su SSD e un ripristino già fatto?	Tre vie in ordine di probabilità, con il motivo
Con quali fonti si costruisce la timeline della notte?	Tabella: fonte, formato delle date, fuso
Che cosa si può attribuire a una persona, e che cosa soltanto a un account?	Due elenchi, come al passo 11 del laboratorio

Quindici minuti in gruppi di tre, poi cinque di confronto. Non c’è un’unica risposta giusta: conta che ogni scelta abbia un motivo scritto.

Quiz di verifica: domande 1–4

1. Un portatile con Windows 11 24H2 è acceso, sbloccato, con il disco cifrato. Per prima cosa

A. lo si spegne e si estrae il disco
B. si acquisiscono la memoria e i dati a volume aperto
C. lo si riavvia da un supporto forense

2. In NTFS, dopo una cancellazione ordinaria, il record del file nella $MFT

A. resta leggibile finché non viene riusato
B. viene azzerato subito
C. viene spostato nel Cestino

3. Un file recuperato con il carving

A. conserva nome e date
B. conserva il nome ma non le date
C. non ha né nome né date di file system

4. Su un SSD interno con TRIM attivo, il contenuto di un file cancellato da giorni

A. con ogni probabilità non è più leggibile
B. si recupera come su un disco magnetico
C. si recupera, purché si usi un write blocker

Quiz di verifica: domande 5–8

5. Nel database History di Chrome le date sono espresse in

A. secondi dal 1970
B. secondi dal 2001
C. microsecondi dal 1601

6. Una data di modifica anteriore a quella di creazione indica di norma

A. un orologio di sistema guasto
B. un file copiato o scaricato
C. un file cifrato

7. La tabella visits ha assegnato nove identificativi e contiene otto righe. Se ne deduce che

A. almeno una visita è stata rimossa
B. il database è corrotto
C. una visita è avvenuta in navigazione privata

8. Secondo la Cassazione del 2025, che cosa si cerca e in quale periodo va indicato

A. nella relazione del consulente
B. al momento dell’estrazione dei dati
C. nel decreto di sequestro

Quiz di verifica: soluzioni

N.	Risposta	Perché
1	B	Spegnendo si perdono la memoria e, senza chiave di ripristino, l’accesso al volume
2	A	La cancellazione segna libero il record; nome, date e posizione dei dati restano
3	C	Il carving riconosce il contenuto dalle firme; nome e date stavano nel record
4	A	Il controller ripulisce i blocchi liberati, anche dietro un write blocker
5	C	Firefox usa i microsecondi dal 1970, Safari i secondi dal 2001
6	B	La copia nasce sul volume di destinazione ma conserva la data di modifica dell’originale
7	A	sqlite_sequence ricorda l’ultimo identificativo assegnato anche dopo una cancellazione
8	C	Cass. n. 34324/2025: la delimitazione non si può rinviare alla fase di estrazione

Sei risposte esatte su otto sono la soglia per ritenere acquisiti i contenuti della giornata.

IN SINTESI

Il disco ricorda più dell’utente, ma meno di una volta: si acquisisce presto, si recupera per livelli, si riferisce ciò che si può sostenere

All’acquisizione

Decidere se spegnere guardando cifratura e memoria. Copiare l’intero supporto, con hash. Annotare fuso e scarto dell’orologio.

In analisi

Cercare i file cancellati dall’alto: copie logiche, record, carving. Portare file system e browser sulla stessa timeline, in UTC.

In relazione

Dire da quale livello viene ogni file recuperato. Separare ciò che è registrato da ciò che è dedotto. Tenere distinto il profilo dalla persona.

SSD e cifratura automatica accorciano ogni anno la finestra utile. Il metodo resta lo stesso; cambia il tempo che si ha per applicarlo.

Fonti: norme, giurisprudenza e standard

Norme e giurisprudenza

- c.p.p., artt. 244, 247, 254-bis, 260, 352, 354, 359 e 360; c.p., art. 615-ter
- L. 18 marzo 2008, n. 48
- Cass. pen., Sez. Un., 20 luglio 2017, n. 40963
- Cass. pen., sez. VI, n. 17479/2025; sez. II, n. 34324/2025; sez. III, n. 41055/2025; sez. VI, n. 40677/2025
- Senato, A.S. 806, e Camera, A.C. 1822, XIX legislatura: art. 254-ter c.p.p.
- Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest, 2001
- Reg. (UE) 2023/1543; Reg. (UE) 2016/679; Dir. (UE) 2016/680; d.lgs. 51/2018
- L. 20 maggio 1970, n. 300, art. 4; Garante per la protezione dei dati personali, Linee guida per posta elettronica e Internet, 1° marzo 2007
- Corte EDU, Grande Camera, Bărbulescu c. Romania, 5 settembre 2017

Standard, linee guida e dati

- ISO/IEC 27037:2012; ISO/IEC 27041:2015, 27042:2015 e 27043:2015
- Kent K. et al., Guide to Integrating Forensic Techniques into Incident Response, NIST SP 800-86, 2006
- Brezinski D., Killalea T., Guidelines for Evidence Collection and Archiving, RFC 3227, 2002
- SWGDE, Best Practices for Computer Forensic Acquisitions, 17-F-002-2.0, 2023
- SWGDE, Best Practices for Computer Forensic Examinations, 18-F-001-2.0
- NIST, Computer Forensics Tool Testing Program
- StatCounter Global Stats, quote di sistemi operativi e browser desktop, ottobre 2026

I riferimenti giurisprudenziali vanno riscontrati sulle banche dati ufficiali prima di essere citati in un atto.

Fonti: letteratura e strumenti

File system, recupero, supporti

- Carrier B., File System Forensic Analysis, Addison-Wesley, 2005
- Farmer D., Venema W., Forensic Discovery, Addison-Wesley, 2005
- Garfinkel S., Carving contiguous and fragmented files with fast object validation, Digital Investigation, 2007
- Pal A., Memon N., The evolution of file carving, IEEE Signal Processing Magazine, 2009
- Bell G., Boddington R., Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?, JDFSL, 2010
- King C., Vidas T., Empirical analysis of solid state disk data retention when used with contemporary operating systems, DFRWS 2011
- Fairbanks K., An analysis of Ext4 for digital forensics, DFRWS 2012
- Hansen K. H., Toolan F., Decoding the APFS file system, Digital Investigation, 2017

Tempo, navigazione, memoria

- Chow K. P. et al., The Rules of Time on NTFS File System, SADFE 2007
- Guðjónsson K., Mastering the Super Timeline with log2timeline, SANS, 2010
- Hargreaves C., Patterson J., An automated timeline reconstruction approach, Digital Investigation, 2012
- Aggarwal G. et al., An analysis of private browsing modes in modern browsers, USENIX Security 2010
- Oh J., Lee S., Lee S., Advanced evidence collection and analysis of web browser activity, Digital Investigation, 2011
- Pawlaszczyk D., Hummert C., Making the invisible visible, 2021
- Ligh M. H. et al., The Art of Memory Forensics, Wiley, 2014
- Vömel S., Freiling F., Correctness, atomicity, and integrity, Digital Investigation, 2012
- Case A., Richard G. G., Memory forensics: The path forward, Digital Investigation, 2017
- Pagani F., Fedorov O., Balzarotti D., Introducing the Temporal Dimension to Memory Forensics, ACM TOPS, 2019
- Strumenti: The Sleuth Kit, Autopsy, foremost, plaso, Volatility 3, AVML, LiME, WinPmem, Hindsight, SQLite

CORSO AVANZATO DI DIGITAL FORENSICS

Grazie per l'attenzione

Vincenzo Calabrò

www.vincenzocalabro.it



Inquadra per aprire il sito