CORSO AVANZATO DI DIGITAL FORENSICS

Acquisizione forense di evidenze dal cloud

Google Drive, iCloud, Microsoft OneDrive, Dropbox e Amazon Web Services: client, account, provider

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 cloud come luogo della prova	30 min
2	Quadro normativo e standard	40 min
	Pausa	15 min
3	Metodo: client, account, provider	50 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 servizio di storage simulato in locale, senza account reali.

Al termine lo studente è in grado di

- distinguere ciò che sta sul client, nell'account e presso il provider, e chi può consegnarlo;
- scegliere la via di acquisizione in base al quesito e al titolo giuridico disponibile;
- acquisire file, versioni e metadati tramite API con strumenti open source, verificandone gli hash;
- esaminare un'acquisizione altrui e riconoscerne i punti contestabili.

PARTE 1 · 30 MINUTI

Il cloud come luogo della prova

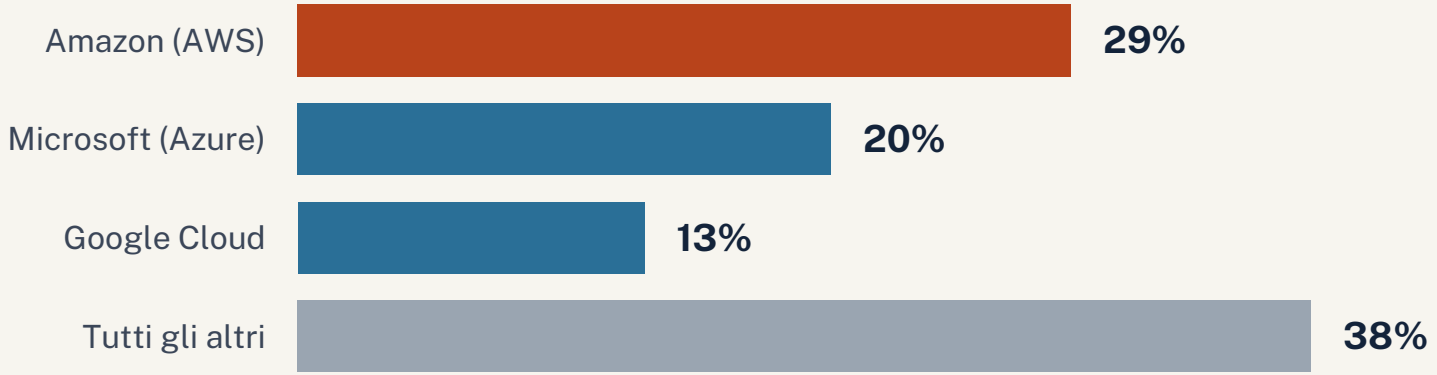
Nel cloud non c’è un disco da sequestrare. Ci sono copie distribuite, regole di conservazione decise dal fornitore e un’interfaccia che mostra soltanto una parte di ciò che esiste.

Il mercato del cloud in numeri

107 mld

di dollari spesi nel mondo in servizi di infrastruttura cloud nel solo terzo trimestre 2025.

Quote di mercato per spesa, terzo trimestre 2025



Conseguenza operativa. Tre fornitori statunitensi raccolgono il 63% della spesa. Chi indaga in Italia si trova quasi sempre a chiedere dati a un soggetto che risponde a un altro ordinamento.

Fonte: Synergy Research Group, dati sul terzo trimestre 2025 pubblicati a novembre 2025. Le quote riguardano l'infrastruttura, non lo storage personale.

Modelli di servizio: chi controlla che cosa

SaaS

Drive, OneDrive, iCloud, Dropbox

Il cliente usa un'applicazione. Vede file, versioni e cronologia nella misura in cui l'interfaccia e le API li espongono. Tutto il resto è del fornitore.

PaaS

Database e funzioni gestite

Il cliente controlla i dati e la configurazione del servizio. Sistema operativo e rete restano invisibili.

IaaS

Amazon Web Services

Il cliente amministra macchine virtuali, dischi, bucket e i relativi log. Può acquisire molto da solo, purché i log fossero stati attivati prima.

Responsabilità condivisa. Più si scende verso l'infrastruttura, più cresce ciò che il cliente può acquisire con le proprie credenziali, e più pesa ciò che aveva o non aveva configurato.

La prima domanda di ogni incarico: quale modello, quindi chi detiene il dato e chi ne detiene i log.

Fonti: NIST SP 800-145, The NIST Definition of Cloud Computing, 2011; NIST SP 800-201, 2024.

Tre luoghi per lo stesso file



I tre luoghi non contengono le stesse cose. Un file «solo online» non è sul client; un log interno non è nell'account.

La volatilità: finestre di conservazione

Servizio	File eliminati	Registro delle attività
Google Drive	Cestino svuotato dopo 30 giorni	Eventi di Drive in Workspace: circa 6 mesi
OneDrive	Cestino: 30 giorni per gli account personali, 93 per quelli aziendali	Audit di Microsoft 365: 180 giorni nel piano standard
iCloud Drive	«Eliminati di recente»: 30 giorni	Nessun registro esposto all'utente
Dropbox	30 giorni nei piani base, 180 nei piani professionali e aziendali	Cronologia eventi; registro attività nei piani aziendali
AWS S3	Senza versioning la cancellazione è immediata	CloudTrail: 90 giorni di eventi di gestione; nulla sugli oggetti, se non configurato

Ogni riga è una scadenza. La richiesta di conservazione al fornitore parte il primo giorno, prima di sapere che cosa servirà.

Valori tipici tratti dalla documentazione dei fornitori, novembre 2026. Variano con il piano e la configurazione: vanno riscontrati caso per caso.

Che cosa occorre poter dimostrare

Contenuto e versioni

Il file com’è oggi e com’era alle date rilevanti: versioni precedenti, elementi nel cestino, oggetti eliminati ma ancora recuperabili.

Chi ha fatto che cosa

Caricamenti, modifiche, condivisioni e cancellazioni, con l’account che le ha compiute, l’indirizzo IP e il dispositivo. È materia di log, non di file.

Tempo

Gli orari attribuiti dal fornitore, in UTC, distinti da quelli che il client scrive sul file locale al momento del download.

Integrità e provenienza

La corrispondenza fra ciò che si produce e ciò che stava nell’account, provata dagli hash che il servizio stesso dichiara e da quelli calcolati dopo l’acquisizione.

Scaricare una cartella risponde alla prima domanda. Le altre tre vivono nei metadati e nei log, che vanno chiesti a parte.

Le vie di acquisizione a confronto

	Contenuto attuale	Versioni e cestino	Log di attività	Senza l’interessato	Dati cifrati dal cliente
Client sincronizzato	In parte	In parte	In parte	In parte	**Sì**
Accesso all’account via API o export	**Sì**	**Sì**	In parte	No	In parte
Richiesta al provider	**Sì**	In parte	**Sì**	**Sì**	No

«In parte» dipende dal servizio e dalla configurazione. Il client conserva soltanto i file sincronizzati; il provider non consegna in chiaro ciò che il cliente ha cifrato con chiavi proprie.

Nessuna via copre tutte le colonne. L’acquisizione dall’account dà i file, la richiesta al provider dà i log: di norma servono entrambe.

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

PARTE 2 · 40 MINUTI

Quadro normativo e standard

Il dato è in un altro Paese, il fornitore in un terzo, l’utente davanti a noi. Il titolo con cui si acquisisce decide quale delle tre vie è percorribile.

Venticinque anni di norme, standard e tecnologia

2001
Convenzione di Budapest sulla criminalità informatica

2008
L. 48/2008: sequestro di dati presso i fornitori (art. 254-bis c.p.p.)

2011
NIST SP 800-145: la definizione di cloud computing

2012
ISO/IEC 27037 sulle prove digitali

2015
Art. 234-bis c.p.p.: dati conservati all'estero

2018
CLOUD Act negli Stati Uniti; GDPR applicabile

2020
NIST IR 8006: le sfide forensi del cloud

2022
Apple introduce Advanced Data Protection per iCloud

2023
Reg. (UE) 2023/1543 e-Evidence; Corte cost. n. 170

2024
NIST SP 800-201: architettura di riferimento forense

2025
SWGDE 23-F-004 v1.1 sull'acquisizione dai provider

2026
e-Evidence applicabile dal 18 agosto

Le norme inseguono un'architettura che cambia più in fretta: per questo gli standard recenti parlano di predisposizione, prima che di acquisizione.

Italia: gli strumenti del codice per i dati nel cloud

Art. c.p.p.	Che cosa consente	Rilievo per il cloud
234-bis	Acquisizione di documenti e dati informatici conservati all'estero, anche non pubblici, con il consenso del legittimo titolare	Accesso con le credenziali fornite dall'interessato
247, co. 1-bis	Perquisizione di sistemi informatici e telematici, con misure che conservino i dati originali	Ricerca sul dispositivo e sui sistemi raggiungibili
254-bis	Sequestro di dati presso i fornitori, anche mediante copia, con obbligo di conservare gli originali	Richiesta al provider
254	Sequestro di corrispondenza	E-mail e messaggi conservati nell'account, dopo Corte cost. n. 170/2023

Cass. pen., sez. VI, n. 18907/2021

Se il detentore collabora spontaneamente, per i dati telematici non occorre la rogatoria, anche ai sensi dell'art. 234-bis.

Cass. pen., sez. VI, n. 44154/2023

Per le comunicazioni già avvenute la norma di riferimento è l'art. 254-bis, non il 234-bis. Chi sia il «legittimo titolare» resta questione discussa.

Fonti: c.p.p. come modificato dalla L. 48/2008 e dal d.l. 7/2015, conv. in L. 43/2015; Corte cost., sent. n. 170/2023. Massime da riscontrare sulle banche dati ufficiali.

Unione europea: dal canale giudiziario al canale diretto

Reg. (UE) 2023/1543

Dal 18 agosto 2026 l'autorità di uno Stato membro rivolge l'ordine di produzione direttamente al fornitore che offre servizi nell'Unione: risposta entro 10 giorni, 8 ore in caso di emergenza.

L'ordine di conservazione blocca i dati per 60 giorni.

Dir. 2014/41/UE

L'ordine europeo di indagine resta la via per gli atti che richiedono l'intervento di un'altra autorità giudiziaria, come la perquisizione di un data center.

Reg. (UE) 2016/679

L'art. 48 ammette il trasferimento di dati personali su ordine di un'autorità di un Paese terzo soltanto se fondato su un accordo internazionale. È il punto di attrito con il CLOUD Act.

Il canale diretto è operativo da pochi mesi. Le categorie di dati, dagli abbonati al contenuto, determinano chi può emettere l'ordine e con quali garanzie.

Fonti: Reg. (UE) 2023/1543 e dir. (UE) 2023/1544; dir. 2014/41/UE; Reg. (UE) 2016/679, art. 48.

Oltre l'Unione: Budapest e CLOUD Act

Convenzione di Budapest

- **Art. 16 e 17**: conservazione rapida dei dati.
- **Art. 18**: ordine di produzione verso chi offre servizi nel territorio.
- **Art. 32, lett. b**: accesso transfrontaliero a dati conservati altrove con il consenso lecito e volontario di chi è legalmente autorizzato a divulgarli.
- **Secondo Protocollo addizionale**, aperto alla firma nel maggio 2022: cooperazione diretta con i fornitori di un altro Stato.

Diritto statunitense

- **Stored Communications Act**: subpoena per i dati di base, ordine del giudice per gli altri record, search warrant per i contenuti.
- **CLOUD Act** (2018): il fornitore soggetto alla giurisdizione statunitense consegna i dati che controlla, ovunque siano conservati.
- **Convenzione ONU** contro la criminalità informatica: adottata il 24 dicembre 2024, aperta alla firma ad Hanoi il 25 ottobre 2025.

Il luogo fisico del dato conta sempre meno. Conta chi lo controlla e a quale ordinamento risponde.

Fonti: Convenzione sulla criminalità informatica, Budapest, 2001; 18 U.S.C. §§ 2701–2713.

Gli standard tecnici per il cloud

NIST SP 800-201 · 2024

Cloud Computing Forensic Reference Architecture. Mette al centro la forensic readiness: predisporre il sistema perché le prove si possano raccogliere in fretta e a costi contenuti.

NIST IR 8006 · 2020

Cloud Computing Forensic Science Challenges. Cataloga le difficoltà proprie del cloud, dalla multi-tenancy alla dispersione geografica dei dati.

SWGDE 23-F-004 v1.1 · 2025

Acquisizione, preservazione e analisi di prove dai cloud service provider. Fra i metodi elenca la richiesta formale al fornitore e, all'estremo opposto, il sequestro fisico dell'hardware.

ISO/IEC 27037:2012

Identificazione, raccolta, acquisizione e conservazione. La Cloud Security Alliance ne ha pubblicato nel 2013 una lettura applicata al cloud.

Tutti convergono su un punto: nel cloud la qualità dell'acquisizione dipende da ciò che era stato predisposto prima dell'incidente.

Fonti: Herman et al., NIST SP 800-201, luglio 2024; NIST IR 8006, agosto 2020; SWGDE 23-F-004-1.1, gennaio 2025; ISO/IEC 27037:2012.

Dal requisito all’artefatto

Requisito	Che cosa lo soddisfa
Autenticità del contenuto	File acquisito tramite API, con l’identificativo dell’oggetto e l’hash dichiarato dal servizio accanto a quello calcolato
Storia del file	Elenco delle versioni con identificativo, data e dimensione; contenuto del cestino; marcatori di cancellazione
Attribuzione	Log di attività e di accesso chiesti al fornitore, dati di registrazione dell’account, dispositivi collegati
Collocazione nel tempo	Orari del servizio in UTC, salvati in un file di metadati separato dal file scaricato
Completezza	Inventario dell’account prima e dopo la copia, con conteggi e dimensioni coincidenti
Legittimità dell’accesso	Provvedimento dell’autorità giudiziaria oppure consenso scritto del titolare, richiamati nel verbale
Ripetibilità	Strumenti a codice aperto, comandi riportati per esteso, versione di ogni programma

La tabella si legge anche al contrario: ogni riga senza artefatto è una domanda che la controparte potrà porre.

PARTE 3 · 50 MINUTI

Metodo e strumenti

Tre vie, dal client al provider, e per ciascun servizio ciò che espone e ciò che nasconde. Gli strumenti sono a codice aperto e si provano nel laboratorio.

Tre vie di acquisizione

1

Dal client

Si acquisisce il dispositivo e si esaminano la cartella sincronizzata, la cache e i database del programma di sincronizzazione.

Dà ciò che era stato sincronizzato, anche a rete spenta. Non dà i file «solo online».

2

Dall’account

Con le credenziali, per consenso o in forza di un provvedimento, si interroga il servizio tramite API oppure si usa la funzione di export.

Dà file, versioni e metadati. È un accesso a un sistema vivo: ogni operazione va registrata.

3

Dal provider

Si rivolge al fornitore una richiesta formale, preceduta da una richiesta di conservazione.

Dà anche i log interni e i dati di registrazione. I tempi sono quelli del fornitore.

Lo studio di Roussev e colleghi del 2016 ha mostrato perché la prima via non basta: revisioni e documenti nativi esistono soltanto nel cloud.

Fonti: SWGDE 23-F-004-1.1, 2025; Roussev, Barreto e Ahmed, API-based forensic acquisition of cloud drives, 2016.

Il client sincronizzato: dove guardare

Servizio	Percorso tipico	Strumento open source
Google Drive	`%LocalAppData%\Google\DriveFS\`	DriveFS Sleuth
OneDrive	`%LocalAppData%\Microsoft\OneDrive\`	OneDriveExplorer
Dropbox	`%LocalAppData%\Dropbox\instance*\`	sqlite3 su sync_history.db
iCloud Drive	`~/Library/Application Support/CloudDocs/`	sqlite3 sui database della sessione

Che cosa si trova. Elenco dei file noti al client, compresi quelli non scaricati; cache dei contenuti aperti; account collegati; tracce di sincronizzazioni e cancellazioni.

Che cosa manca. Le versioni precedenti, le condivisioni viste dal lato del servizio, i log di accesso. Formati e percorsi cambiano con le versioni del client.

Percorsi da riscontrare sulla versione installata. Fonti: documentazione di DriveFS Sleuth e OneDriveExplorer; repository ForensicArtifacts.

Google Drive: file, revisioni e documenti nativi

Dall’account

L’API elenca ogni file con identificativo, proprietario, date di creazione e modifica, permessi e, per i file binari, gli hash MD5, SHA-1 e SHA-256.

Le revisioni si elencano e si scaricano una per una.

Documenti nativi

Documenti, Fogli e Presentazioni non sono file: esistono soltanto nel servizio. Si esportano in un formato scelto, e l’export non ha un hash dichiarato da Google.

Due export dello stesso documento possono differire.

Export e ambito aziendale

Takeout consegna all’utente un archivio dei propri dati. In Workspace l’amministratore dispone di Vault per conservazione ed export e del registro degli eventi di Drive.

Il registro risponde alla domanda «chi ha fatto che cosa».

Per un documento nativo la prova è la cronologia delle revisioni nel servizio. Il file esportato ne è una fotografia, datata al momento dell’export.

Fonti: documentazione di Google Drive API v3, Google Takeout e Google Vault, consultata a novembre 2026.

Microsoft OneDrive: due servizi sotto lo stesso nome

OneDrive personale

Legato a un account Microsoft privato. File, versioni e cestino si raggiungono con le credenziali dell'utente tramite Microsoft Graph.

Il Personal Vault richiede una seconda verifica dell'identità e si richiude da solo dopo un periodo di inattività.

OneDrive aziendale

È una raccolta SharePoint dentro un tenant Microsoft 365. L'amministratore dispone di Purview per ricerca, conservazione ed export, e del registro di audit unificato.

Cestino a due livelli; conservazione dell'audit di 180 giorni nel piano standard.

Hash. Microsoft Graph espone per ogni file un quickXorHash, algoritmo proprio di Microsoft; SHA-1 e SHA-256 compaiono soltanto in alcuni tipi di account. L'hash crittografico va quindi calcolato dopo il download.

In ambito aziendale il primo interlocutore è l'amministratore del tenant: molte acquisizioni si fanno senza coinvolgere Microsoft.

Fonti: documentazione di Microsoft Graph (risorsa driveItem) e di Microsoft Purview, consultata a novembre 2026.

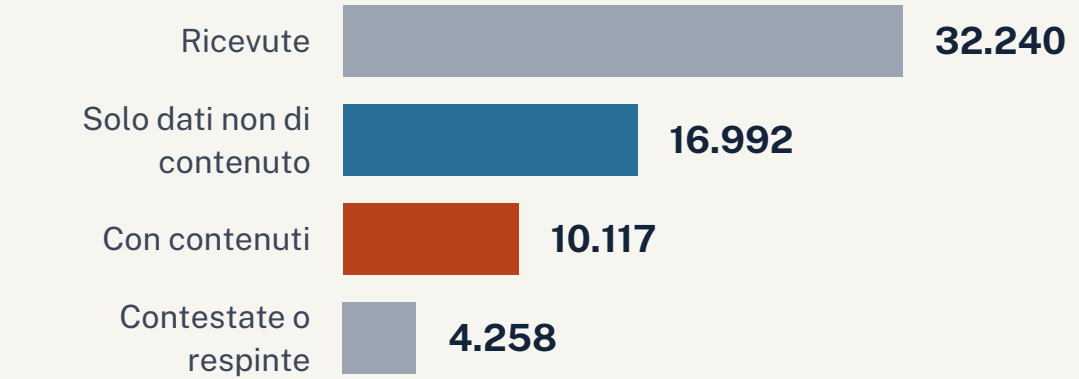
iCloud: ciò che Apple può consegnare, e quando non può

Protezione standard. Apple conserva le chiavi della maggior parte dei dati: con il titolo adeguato può consegnare contenuti come foto, backup dei dispositivi, contatti e calendari.

Advanced Data Protection. Introdotta a fine 2022 e facoltativa, estende la cifratura end-to-end a backup, iCloud Drive e Foto. Le chiavi restano sui dispositivi dell'utente: Apple non può decifrare.

Dall'account. L'utente ottiene una copia dei propri dati dal portale privacy di Apple. I tempi sono di giorni, non di minuti.

Richieste di dati di account ricevute da Apple nel mondo, luglio–dicembre 2025



Dall'Italia: 139 richieste su 187 account; dati forniti nel 24% dei casi, mai contenuti.

Prima di scrivere ad Apple conviene sapere se l'account ha la protezione avanzata attiva: lo si legge sul dispositivo.

Fonti: Apple Transparency Report, luglio–dicembre 2025; documentazione Apple su Advanced Data Protection.

Dropbox: cronologia delle versioni e hash a blocchi

Versioni ed eventi

Ogni file conserva le versioni precedenti per la durata prevista dal piano. La pagina degli eventi elenca aggiunte, modifiche, cancellazioni e condivisioni.

Hash dichiarato

L'API restituisce per ogni file un content_hash: il file è diviso in blocchi da 4 MB, di ciascuno si calcola lo SHA-256, e l'hash finale è lo SHA-256 della loro concatenazione.

Non coincide con lo SHA-256 del file.

Ambito aziendale

L'amministratore del team vede il registro delle attività dei membri e può accedere ai loro contenuti nei limiti delle policy interne.

In pratica. Per verificare un file scaricato rispetto a ciò che Dropbox dichiara occorre ricalcolare il content_hash con lo stesso algoritmo; strumenti come rclone lo fanno in automatico.

Un hash diverso dallo SHA-256 atteso non indica un'alterazione: indica un algoritmo diverso.

Fonti: documentazione dell'API di Dropbox (Content hash) e del centro assistenza, consultata a novembre 2026.

Amazon Web Services: il cliente come primo acquisitore

Servizio	Che cosa conserva	Condizione
S3	Oggetti, versioni precedenti, marcatori di cancellazione	Versioning attivato sul bucket prima dei fatti
CloudTrail	Chiamate alle API: chi, quando, da quale indirizzo IP	90 giorni per gli eventi di gestione; gli eventi sugli oggetti solo se il trail li registra
EBS	Snapshot dei dischi delle macchine virtuali	Lo snapshot si crea al momento dell'acquisizione
IAM	Utenti, ruoli, chiavi di accesso e data dell'ultimo utilizzo	Sempre disponibile all'amministratore
Log di rete e di accesso	VPC Flow Logs, log di accesso ai bucket	Soltanto se abilitati in precedenza

In AWS quasi tutto si acquisisce con le credenziali del cliente. Ciò che non era stato attivato prima dell'incidente non esiste, e nessuna richiesta ad Amazon lo farà comparire.

Fonti: documentazione AWS di S3, CloudTrail, EBS e IAM; AWS Security Incident Response User Guide. Consultate a novembre 2026.

Che cosa può consegnare il provider

	Contenuto dei file	Dati di registrazione	Log di accesso e attività	Dati cifrati dal cliente
Google	**Sì**	**Sì**	**Sì**	No
Microsoft	**Sì**	**Sì**	**Sì**	No
Apple	In parte	**Sì**	In parte	No
Dropbox	**Sì**	**Sì**	**Sì**	No
Amazon Web Services	In parte	**Sì**	In parte	No

- **Apple**: «in parte» perché con Advanced Data Protection attiva i contenuti non sono decifrabili dal fornitore.
- **AWS**: «in parte» perché oggetti e log appartengono al cliente, che spesso li cifra con chiavi proprie e ne decide la conservazione.
- **Per tutti**: il contenuto richiede il titolo più forte previsto dall'ordinamento del fornitore.

Sintesi di quanto i fornitori dichiarano nelle linee guida per le autorità e nei rapporti di trasparenza. Il risultato dipende dal titolo giuridico.

Integrità: gli hash che il servizio dichiara

Servizio	Hash esposto dall'API	Avvertenza
Google Drive	MD5, SHA-1 e SHA-256 del file	Assenti per Documenti, Fogli e Presentazioni nativi
OneDrive	quickXorHash; SHA-1 o SHA-256 in alcuni account	quickXorHash non è un hash crittografico
Dropbox	content_hash, SHA-256 calcolato a blocchi	Diverso dallo SHA-256 dell'intero file
AWS S3	ETag; checksum aggiuntivi se richiesti al caricamento	L'ETag coincide con l'MD5 soltanto per i caricamenti in un solo pezzo
iCloud Drive	Nessun hash documentato per l'utente	Resta soltanto l'hash calcolato dopo il download

Due hash, due funzioni. Quello del servizio prova che la copia coincide con ciò che stava nell'account. Quello calcolato in proprio sigilla la copia da quel momento in poi.

A verbale. Algoritmo, valore dichiarato, valore calcolato, esito del confronto, per ogni file. Senza il primo valore il confronto non si può più rifare.

Fonti: documentazione delle API dei cinque servizi, consultata a novembre 2026. I campi disponibili cambiano con il tipo di account.

La cassetta degli strumenti open source

Strumento	A che cosa serve	Limite da conoscere
rclone	Inventario, copia e verifica via API su Drive, OneDrive, Dropbox, S3 e decine di altri servizi	Le funzioni disponibili dipendono dalla versione e dal servizio
AWS CLI	Interrogazione diretta delle API di AWS: versioni, log, snapshot	Opera con i permessi delle credenziali usate
DriveFS Sleuth	Analisi degli artefatti locali di Google Drive per desktop	Legato al formato della versione del client
OneDriveExplorer	Ricostruzione dell'albero di OneDrive dai file del client	Legato al formato della versione del client
kumodd	Prototipo di ricerca per l'acquisizione via API, revisioni comprese	Nato nel 2016: va verificato sulle API attuali
sha256sum, tar, ots	Hash, archivio e marca temporale del fascicolo	La marca OpenTimestamps non è qualificata ai sensi di eIDAS

Uno strumento che usa le API ufficiali vede ciò che il fornitore ha deciso di mostrare. Il suo registro delle operazioni fa parte dell'acquisizione.

Fonti: documentazione dei progetti (rclone.org, AWS CLI, DriveFS Sleuth, OneDriveExplorer, kumodd, OpenTimestamps).

I limiti dell’acquisizione tramite API

Copia logica

Non esiste un’immagine bit a bit dell’account. Si ottiene ciò che il servizio restituisce a quella richiesta, in quel momento, con quei permessi.

Orari

Quick e Choo (2013) hanno verificato che il contenuto dei file scaricati resta identico, mentre le date sul file locale cambiano secondo il metodo di download. Gli orari validi sono quelli dichiarati dal servizio.

Tracce dell’esaminatore

L’accesso lascia nel registro dell’account una sessione, un indirizzo IP, talvolta una notifica all’utente. Vanno annotati per distinguerli dall’attività indagata.

Sistema vivo

Durante la copia l’account può cambiare: altri dispositivi sincronizzano, i timer del cestino scadono. Due inventari, prima e dopo, misurano la differenza.

Un’acquisizione dal cloud si descrive per ciò che è: una copia logica, mediata dal fornitore, di un sistema in esercizio.

Fonti: Quick e Choo, Digital Investigation 10(3), 2013; Roussev, Barreto e Ahmed, 2016; SWGDE 23-F-004-1.1.

PARTE 4 · 70 MINUTI

Laboratorio guidato

Dall’inventario al fascicolo sigillato, con strumenti a codice aperto. Le schermate provengono da un servizio S3 simulato in locale: nessun account reale è stato usato.

Scenario e regole del laboratorio

Scenario

Uno studio professionale conserva le pratiche in un bucket di storage. Un contratto non si trova più: l'elenco dei file non lo mostra, e un collaboratore sostiene che non sia mai stato caricato.

Quesito. Stabilire se il file è esistito, in quante versioni e quando è stato eliminato, e recuperarne il contenuto.

Cartella di lavoro: caso03. Bucket di prova: studio-prova, con tre file di fantasia.

Regole

Il servizio è simulato sulla postazione con moto, una libreria che riproduce le API di S3. Credenziali e contenuti sono fittizi.

Sul servizio si eseguono soltanto operazioni di lettura. Ogni comando finisce a verbale con data e ora in UTC.

Le stesse operazioni, su un account reale, richiedono un titolo: consenso scritto o provvedimento.

Sette passi, dieci minuti ciascuno. A ogni passo corrisponde una riga del verbale.

Passo 1: la postazione

INSTALLAZIONE SU UBUNTU 24.04

```
$ sudo apt install rclone sqlite3
$ python3 -m venv ~/venv-cloud
$ ~/venv-cloud/bin/pip install awscli "moto[server]"
$ ~/venv-cloud/bin/moto_server -H 127.0.0.1 -p 5000 &
```

VERSIONI, DA RIPORTARE A VERBALE

```
$ rclone version ; aws --version
# rclone v1.60.1 · aws-cli/1.46.3 · moto 5.2.6
```

Il simulatore. I client puntano all'indirizzo locale tramite il parametro endpoint dei rispettivi file di configurazione. I comandi sono identici a quelli che si userebbero su AWS.

Il limite. Il simulatore riproduce S3, non CloudTrail né i servizi di Google, Microsoft, Apple e Dropbox: per quelli il laboratorio indica i comandi senza eseguirli.

Comandi eseguiti il 28 novembre 2026 su Ubuntu 24.04 nella preparazione del corso.

Passo 2: ricognizione dell’account

CHI SONO, DOVE SONO, CHE COSA È ATTIVO

```
$ date -u +%Y-%m-%dT%H:%M:%SZ
$ aws sts get-caller-identity
$ aws s3api get-bucket-location --bucket studio-prova
$ aws s3api get-bucket-versioning --bucket studio-prova
# eu-south-1 · Enabled
```

Identità

Il primo comando dopo l’orologio dichiara con quale utenza si sta operando. È la riga che lega ogni risultato successivo a un titolo di accesso.

Regione

Dice in quale Paese risiedono i dati: nel caso di prova la regione di Milano. Entra nel verbale perché orienta le questioni di giurisdizione.

Versioning

«Enabled» significa che le sovrascritture e le cancellazioni hanno lasciato traccia. Se fosse stato sospeso, il laboratorio finirebbe qui.

Comandi eseguiti sul servizio simulato il 28 novembre 2026. L’utenza restituita dal simulatore è fittizia.

Passo 3: ciò che l’elenco non mostra

```
studente@vm:~/caso03$ aws s3 ls s3://studio-prova --recursive
2026-11-28 18:35:32         35 pratiche/fornitori.csv
2026-11-28 18:35:32         43 pratiche/verbale.txt
studente@vm:~/caso03$ Q="[VersionId,IsLatest,LastModified,Size,ETag]"
studente@vm:~/caso03$ aws s3api list-object-versions --bucket studio-prova --prefix pratiche/contratto --output text --query "Versions[].$Q"
69cbc519-457b-4136-bfdd-d45272b06ce9    False   2026-11-28T17:35:36.000Z        57      "6e7383c18d830690a19702910b7be741"
d16de127-2ea9-4a5e-983d-e13cb0bcf2fe    False   2026-11-28T17:35:33.000Z        45      "0b044e5d01740844c0ef3b718a6eba9c"
studente@vm:~/caso03$ aws s3api list-object-versions --bucket studio-prova --prefix pratiche/contratto --output text --query "DeleteMarkers[
].[VersionId,IsLatest,LastModified]"
cf1802f2-37b5-4330-bc0c-31347337dbaf    True    2026-11-28T17:35:39.000Z
studente@vm:~/caso03$
```

L’elenco ordinario. Mostra due file. Il contratto non c’è, e gli orari sono espressi nell’ora locale della postazione.

L’elenco delle versioni. Per la stessa chiave esistono due versioni, di 45 e di 57 byte, caricate a tre secondi di distanza, e un marcatore di cancellazione successivo. Qui gli orari sono in UTC.

Il file è esistito in due versioni ed è stato eliminato dopo la seconda. In un bucket con versioning la cancellazione aggiunge un marcatore; non rimuove nulla.

Schermata originale, prodotta il 28 novembre 2026 su un servizio S3 simulato in locale con dati di fantasia.

Passo 4: recuperare una versione e verificarla

DOWNLOAD DI UNA VERSIONE PRECISA

```
$ aws s3api get-object --bucket studio-prova --key pratiche/contratto.txt \
    --version-id d16de127-2ea9-4a5e-983d-e13cb0bcf2fe recuperato/contratto_v1.txt
# "LastModified": "Sat, 28 Nov 2026 17:35:33 GMT", "ContentLength": 45,
# "ETag": "\"0b044e5d01740844c0ef3b718a6eba9c\"", "VersionId": "d16de127-…"
$ md5sum recuperato/contratto_v1.txt
# 0b044e5d01740844c0ef3b718a6eba9c recuperato/contratto_v1.txt
```

La risposta del servizio è un reperto. Il JSON restituito da get-object contiene data, dimensione, ETag e identificativo della versione: si salva in un file accanto al contenuto.

Il confronto. Per un oggetto caricato in un solo pezzo l'ETag è l'MD5 del contenuto: i due valori coincidono. Poi si calcola lo SHA-256, che il servizio non dichiara.

La richiesta della chiave senza versione restituisce «404 Not Found»: lo stesso oggetto esiste o non esiste secondo la domanda che si pone.

Comandi e risultati ottenuti sul servizio simulato il 28 novembre 2026.

Passo 5: copia completa e verifica con rclone

```
studente@vm:~/caso03$ rclone lsl --s3-versions cloud:studio-prova
       57 2026-11-28 18:35:36.000000000 pratiche/contratto-v2026-11-28-173536-000.txt
       45 2026-11-28 18:35:33.000000000 pratiche/contratto-v2026-11-28-173533-000.txt
       35 2026-11-28 18:35:32.000000000 pratiche/fornitori.csv
       43 2026-11-28 18:35:32.000000000 pratiche/verbale.txt
studente@vm:~/caso03$ rclone copy --s3-versions cloud:studio-prova acquisizione/
studente@vm:~/caso03$ rclone check --s3-versions cloud:studio-prova acquisizione/
2026/11/28 18:36:22 NOTICE: Local file system at /home/studente/caso03/acquisizione: 0 differences found
2026/11/28 18:36:22 NOTICE: Local file system at /home/studente/caso03/acquisizione: 4 matching files
studente@vm:~/caso03$ md5sum acquisizione/pratiche/* | tee acquisizione.md5
0b044e5d01740844c0ef3b718a6eba9c  acquisizione/pratiche/contratto-v2026-11-28-173533-000.txt
6e7383c18d830690a19702910b7be741  acquisizione/pratiche/contratto-v2026-11-28-173536-000.txt
e9c49218717e06166bd2b2cfccdf07ad  acquisizione/pratiche/fornitori.csv
75253ae1ffd54f6e109e83b288c01e7b  acquisizione/pratiche/verbale.txt
studente@vm:~/caso03$
```

Inventario e copia. Con --s3-versions rclone tratta ogni versione come un file a sé, con la data nel nome. La copia conserva gli orari di modifica dichiarati dal servizio.

Verifica. rclone check confronta dimensione e hash di ogni file con quelli remoti: zero differenze, quattro corrispondenze. L’elenco degli MD5 locali finisce in un file del fascicolo.

Schermata originale del 28 novembre 2026, rclone 1.60.1 su servizio S3 simulato. Gli MD5 coincidono con gli ETag del passo 3.

Passo 6: lo stesso metodo su Drive, OneDrive e Dropbox

CON UN ACCOUNT DI PROVA E L'AUTORIZZAZIONE DEL TITOLARE

```
$ rclone config
$ rclone lsjson -R --hash drive: > inventario-prima.json
$ rclone copy drive: acquisizione-drive/ --drive-export-formats docx,xlsx,pptx \
    --log-file rclone.log -v
$ rclone check drive: acquisizione-drive/
$ rclone lsjson -R --hash drive: > inventario-dopo.json
```

Sola lettura

In fase di configurazione si sceglie l'ambito di accesso in sola lettura: lo strumento non potrà modificare l'account neppure per errore.

Documenti nativi

Vengono esportati nei formati indicati. Non avendo hash remoto, la verifica li segnala come non confrontabili: è corretto, e va spiegato.

Due inventari

Il confronto fra il JSON di prima e quello di dopo mostra se l'account è cambiato durante la copia.

Sintassi tratta dalla documentazione di rclone. Comandi non eseguiti nella preparazione del corso: richiedono un account reale.

Passo 7: chi ha eliminato il file

CLOUDTRAIL, SU UN ACCOUNT AWS REALE

```
$ aws cloudtrail describe-trails
$ aws cloudtrail get-event-selectors --trail-name <nome-del-trail>
$ aws cloudtrail lookup-events --start-time 2026-11-01T00:00:00Z \
    --lookup-attributes AttributeKey=ResourceName,AttributeValue=studio-prova
```

Eventi di gestione

Creazione del bucket, modifica del versioning, cambi di policy. Sono registrati di default e consultabili per 90 giorni con lookup-events.

Eventi sui dati

Lettura, scrittura e cancellazione dei singoli oggetti. Esistono soltanto se un trail era stato configurato per registrarli: il secondo comando lo verifica.

Il marcatore di cancellazione dice quando. Chi, e da quale indirizzo, lo dice soltanto un log che qualcuno aveva deciso di tenere.

Sintassi tratta dalla documentazione di AWS CLI. Comandi non eseguiti: il simulatore non riproduce CloudTrail.

Chiusura: il fascicolo e il sigillo

Che cosa contiene il fascicolo

- Inventario dell’account prima e dopo la copia.
- Risposte del servizio in JSON, comprese quelle di errore.
- File acquisiti, con tutte le versioni.
- Elenco degli hash dichiarati e di quelli calcolati.
- Registro delle operazioni dello strumento.
- Verbale con titolo di accesso, utenza, orari in UTC.

SIGILLO

```
$ find caso03 -type f -exec sha256sum {} + \
    | tee caso03.sha256
$ tar -cf caso03.tar caso03 caso03.sha256
$ sha256sum caso03.tar
$ ots stamp caso03.tar
```

La marca OpenTimestamps prova che l’archivio esisteva a una certa data. Dove occorre l’efficacia prevista da eIDAS si aggiunge una marca temporale qualificata.

Fonti: Reg. (UE) n. 910/2014, artt. 41 e 42; documentazione di OpenTimestamps.

Errori ricorrenti

Errore	Conseguenza
Rimandare la richiesta di conservazione al fornitore	Cestino e log scadono mentre si discute del titolo
Scaricare i file dal browser, uno per uno	Nessun metadato, nessun hash dichiarato, orari del download al posto di quelli reali
Fermarsi all'elenco ordinario dei file	Versioni precedenti e oggetti eliminati restano invisibili
Usare credenziali con permessi di scrittura	Rischio di modificare l'account e di doverlo spiegare
Confrontare hash di algoritmi diversi	Falsi allarmi di alterazione su file integri
Trattare un documento nativo esportato come l'originale	Si perde la cronologia delle revisioni, che era la prova
Chiedere i log dopo i file	Per molti servizi i log durano meno dei file
Accedere con credenziali trovate sul dispositivo, senza titolo	Acquisizione inutilizzabile e possibile accesso abusivo

Il primo e l'ultimo errore non sono tecnici: si commettono prima di aprire un terminale.

Limiti legali ed etici

Il titolo

In sede penale, provvedimento dell’autorità giudiziaria. In sede privata, consenso scritto e informato del titolare dell’account, che indichi quali dati e per quale scopo.

Le credenziali trovate

Una password salvata nel dispositivo sequestrato non autorizza da sola a entrare nell’account. L’accesso al cloud deve essere coperto dal titolo in modo espresso.

I terzi

Cartelle condivise e spazi aziendali contengono dati di persone estranee al procedimento. Si acquisisce ciò che serve al quesito e si documenta il criterio di selezione.

La corrispondenza

Se nell’account ci sono e-mail o messaggi, valgono le garanzie del sequestro di corrispondenza. L’accesso senza titolo può integrare gli artt. 615-ter e 616 c.p.

Su dati altrui serve un titolo, e la sua valutazione spetta a un legale.

Riferimenti: artt. 15 Cost., 615-ter e 616 c.p., 234-bis, 254 e 254-bis c.p.p.; Reg. (UE) 2016/679. Indicazioni didattiche, non pareri legali.

PARTE 5 · 35 MINUTI

Caso di studio e verifica

Un fascicolo da esaminare in gruppo, otto domande a risposta chiusa, la sintesi e le fonti.

Caso di studio: i progetti dell’ex dipendente

Scenario di fantasia

Una società sospetta che un progettista, prima delle dimissioni, abbia copiato disegni riservati dallo spazio aziendale a un proprio account personale. Il progettista nega. La società ha un tenant Microsoft 365 e alcuni bucket su AWS.

Incarico. Come consulenti della società, valutare ciò che è agli atti e indicare che cosa manca.

Che cosa c’è nel fascicolo

N.	Reperto
1	Cartella di disegni scaricata dal browser dall’amministratore, senza hash
2	Immagine forense del portatile aziendale, con il client di sincronizzazione
3	Export del registro di audit del tenant, ultimi 30 giorni
4	Elenco ordinario degli oggetti di un bucket, senza versioni
5	Schermata della pagina di condivisione di una cartella

Le dimissioni risalgono a quattro mesi fa. Nessuna richiesta di conservazione è stata inviata.

Caso di studio: il lavoro in gruppo

1

Per ciascun reperto, a quali delle quattro domande risponde: contenuto e versioni, chi ha fatto che cosa, tempo, integrità?

2

Quali fonti sono ancora recuperabili a quattro mesi dai fatti, e quali sono con ogni probabilità scadute? Con quale ordine di priorità si procede?

3

Che cosa può dire il reperto 2 sulla copia verso un account personale, e che cosa non potrà mai dire?

4

Che cosa si può acquisire con i soli poteri dell'amministratore, che cosa richiede il fornitore, e che cosa richiede l'autorità giudiziaria?

Venti minuti in gruppi di tre, poi tre minuti di restituzione per gruppo. La risposta attesa è una tabella, non un racconto.

Quiz di verifica: domande 1–4

1. In un bucket S3 con versioning attivo, cancellare un oggetto

A. rimuove tutte le sue versioni
B. aggiunge un marcatore di cancellazione e conserva le versioni
C. lo sposta in un cestino per trenta giorni

2. L’art. 234-bis c.p.p. consente di acquisire dati non pubblici conservati all’estero

A. con il consenso del legittimo titolare
B. in ogni caso, senza condizioni
C. soltanto mediante rogatoria

3. Il content_hash restituito da Dropbox è

A. lo SHA-256 dell’intero file
B. l’MD5 del file
C. uno SHA-256 calcolato sui blocchi da 4 MB

4. Un documento nativo di Google Documenti

A. ha un MD5 dichiarato dal servizio
B. non ha hash dichiarato e si esporta in un formato scelto
C. non si può acquisire tramite API

Quiz di verifica: domande 5–8

5. Con Advanced Data Protection attiva, per i backup di iCloud Apple

A. consegna i contenuti a fronte di un search warrant
B. consegna i contenuti soltanto alle autorità europee
C. non dispone delle chiavi per decifrarli

6. Per CloudTrail la cancellazione di un oggetto S3 è

A. un evento sui dati, registrato soltanto se un trail lo prevede
B. un evento di gestione, sempre registrato
C. un'operazione che non si può registrare

7. Dal 18 agosto 2026 il Reg. (UE) 2023/1543

A. sostituisce l'ordine europeo di indagine
B. consente ordini di produzione diretti ai fornitori, con risposta in dieci giorni
C. riguarda soltanto i dati degli abbonati

8. Il client di sincronizzazione su un portatile sequestrato

A. contiene tutte le versioni di ogni file
B. contiene i log di accesso del fornitore
C. contiene ciò che è stato sincronizzato, non i file «solo online»

Quiz di verifica: soluzioni

N.	Risposta	Perché
1	B	È ciò che si è visto nel laboratorio: l’elenco ordinario tace, le versioni restano
2	A	Il consenso è la condizione posta dalla norma per i dati non pubblici
3	C	Per questo non coincide con lo SHA-256 del file
4	B	Non è un file: esiste soltanto nel servizio, con la sua cronologia
5	C	Le chiavi restano sui dispositivi dell’utente
6	A	Senza quella configurazione il log non esiste
7	B	Otto ore nei casi di emergenza; l’ordine europeo di indagine resta in vigore
8	C	Versioni e log stanno nell’account e presso il fornitore

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

IN SINTESI

Dal cloud si acquisisce una copia logica di un sistema vivo: il metodo sta nel documentare che cosa si è chiesto, a chi e con quale titolo

Prima di toccare

Individuare modello di servizio e detentore dei dati. Inviare la richiesta di conservazione. Verificare che il titolo copra l'accesso all'account.

Durante

Operare in sola lettura tramite API. Acquisire versioni, cestino e metadati, oltre ai file. Salvare gli hash dichiarati accanto a quelli calcolati.

Dopo

Chiedere al fornitore i log che l'account non mostra. Dichiarare i limiti: che cosa non era attivo, che cosa era scaduto, che cosa è cifrato.

Nel cloud ciò che non è stato predisposto prima non si recupera dopo. Vale per chi indaga e per chi vuole potersi difendere.

Fonti: norme, giurisprudenza e standard

Norme e giurisprudenza

- C.p.p., artt. 234-bis, 247, 254, 254-bis; c.p., artt. 615-ter e 616; Costituzione, art. 15
- L. 18 marzo 2008, n. 48; d.l. 18 febbraio 2015, n. 7, conv. in L. 43/2015
- Corte cost., sent. 27 luglio 2023, n. 170
- Cass. pen., sez. VI, n. 18907/2021; sez. VI, n. 44154/2023
- Reg. (UE) 2023/1543 e dir. (UE) 2023/1544; dir. 2014/41/UE
- Reg. (UE) 2016/679, art. 48; Reg. (UE) n. 910/2014, artt. 41 e 42
- Convenzione sulla criminalità informatica, Budapest, 2001, e Secondo Protocollo addizionale, 2022
- Stored Communications Act e CLOUD Act, 18 U.S.C. §§ 2701–2713
- Convenzione ONU contro la criminalità informatica, 2024

Standard e linee guida

- Herman M. et al., NIST Cloud Computing Forensic Reference Architecture, NIST SP 800-201, luglio 2024
- NIST Cloud Computing Forensic Science Challenges, NIST IR 8006, agosto 2020
- Mell P., Grance T., The NIST Definition of Cloud Computing, NIST SP 800-145, 2011
- SWGDE, Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers, 23-F-004-1.1, gennaio 2025
- ISO/IEC 27037:2012
- Cloud Security Alliance, Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing, 2013

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

Fonti: letteratura, documentazione e strumenti

Letteratura scientifica

- Ruan K., Carthy J., Kechadi T., Crosbie M., Cloud forensics, Advances in Digital Forensics VII, 2011
- Chung H., Park J., Lee S., Kang C., Digital forensic investigation of cloud storage services, Digital Investigation 9(2), 2012
- Martini B., Choo K.-K. R., An integrated conceptual digital forensic framework for cloud computing, Digital Investigation 9(2), 2012
- Quick D., Choo K.-K. R., Dropbox analysis: Data remnants on user machines, Digital Investigation 10(1), 2013
- Quick D., Choo K.-K. R., Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?, Digital Investigation 10(3), 2013
- Quick D., Choo K.-K. R., Google Drive: Forensic analysis of data remnants, Journal of Network and Computer Applications 40, 2014
- Roussev V., Barreto A., Ahmed I., API-based forensic acquisition of cloud drives, Advances in Digital Forensics XII, 2016
- Roussev V., McCulley S., Forensic analysis of cloud-native artifacts, Digital Investigation 16, 2016

Documentazione e dati

- Apple, Transparency Report, luglio–dicembre 2025
- Synergy Research Group, quote di mercato del terzo trimestre 2025
- Documentazione di Google Drive API, Microsoft Graph, Dropbox API, AWS S3 e CloudTrail

Strumenti

- rclone, rclone.org
- AWS CLI; moto, simulatore delle API di AWS
- DriveFS Sleuth; OneDriveExplorer; kumodd
- OpenTimestamps

Autori, volumi e pagine vanno riscontrati sulle pagine degli editori prima della citazione.

CORSO AVANZATO DI DIGITAL FORENSICS

Grazie per l'attenzione

Vincenzo Calabrò

www.vincenzocalabro.it



Inquadra per aprire il sito