Acquisizione logica di dispositivi iOS: tipologie, analisi e differenze nelle modalità e nei dati estratti - parte I

Author : Luca Cadonici

Date : 14 Settembre 2020

Nonostante nell'ultimo anno si sia assistito allo sviluppo di tecniche sempre più efficaci per l'acquisizione fisica dei dispositivi mobili Apple[1], le modalità logiche di acquisizione di iOS restano ancora una soluzione spesso obbligata - e talvolta consigliata - al fine di ridurre al minimo le possibilità di danneggiamento dei dispositivi da periziare.

Notevole è infatti la quantità di dati acquisibili utilizzando i servizi propri dell'azienda di Cupertino, quali backup iTunes e iCloud, soprattutto in rapporto a soluzioni "native" di altre case madri quali Huawei o Samsung e, ancora di più, dei backup Android. A patto che il codice di accesso al dispositivo e di eventuale cifratura del backup sia noto, l'acquisizione logica consente l'immediato accesso a dati di primario interesse investigativo e riduce al minimo l'impatto sui dati memorizzati, utilizzando i servizi proposti dalla stessa casa di produzione e limitandosi all'analisi dei dati estratti, di norma già decifrati come nel caso delle chat WhatsApp, normalmente protette da cifratura *end-to-end*.

Possiamo individuare essenzialmente **tre tipologie** di acquisizione logica per i dispositivi iOS, cioè tre tipi di acquisizione che riflettano il contenuto preciso di un dispositivo fisico, escludendo quindi i dati sincronizzati con iCloud e i file memorizzati nello *storage* cloud di Apple:

1. iTunes backup;
2. iTunes encrypted backup;
3. iCloud backup.

Apple supporta infatti due tipologie principali di backup, ognuna con le proprie specificità in merito alle procedure di acquisizione e alla quantità di dati estratti: locale (tramite iTunes) e su iCloud.

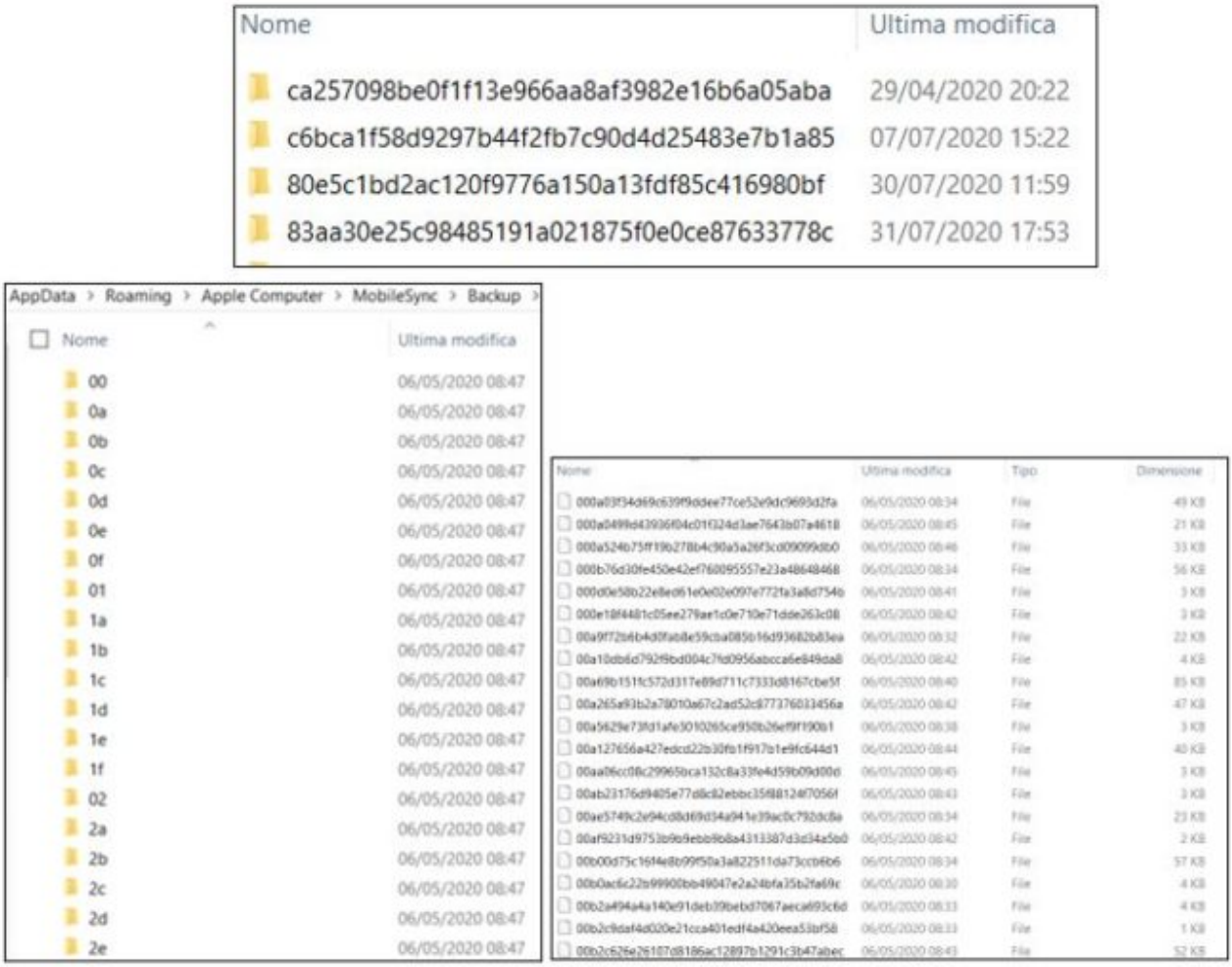
La prima permette di realizzare backup eventualmente cifrati del proprio dispositivo su PC o Mac, la seconda sfrutta il servizio di *storage* Cloud di Apple per realizzare backup cifrati dei dispositivi iOS tramite connessione Wi-Fi utilizzando parte dei 5GB gratuiti offerti ad ogni utente, aumentabili fino a 2 TB tramite apposito abbonamento.

iTunes backup

Il backup locale tramite *iTunes* viene creato automaticamente al momento della sincronizzazione tra il dispositivo iOS e la workstation a cui viene connesso, pertanto è consigliabile disattivare la sincronizzazione automatica dei dispositivi nella configurazione di iTunes al fine di non interferire con i reperti in fase di acquisizione. Alternativamente, è possibile creare manualmente il backup dei dispositivi associati tramite click sul nome del dispositivo in iTunes e selezione dell'apposita opzione. In tal caso, però, il nostro nome utente rimarrà memorizzato come quello dell'ultima sincronizzazione.

I backup di iOS hanno alcune caratteristiche e limitazioni che li contraddistinguono. Ovvero:

- non è possibile scegliere quali dati includere nel backup. iTunes crea sempre una copia quasi completa dell'intero dispositivo, a differenza ad esempio dei backup Samsung e Huawei;
- il backup non viene archiviato in un unico singolo file; iTunes crea diversi file in un formato proprietario in cui i dati memorizzati non sono immediatamente leggibili. Gli utenti possono ripristinare i file solo su un dispositivo iOS (o in un software forense) che assembla i file contenuti nelle varie cartelle in modo da ricomporre i dati originali;
- il backup può essere protetto con una password scelta dall'utente, permettendo l'inclusione di "dati sensibili" aggiuntivi altrimenti non presenti;
- i backup di iPhone, iPad o iPod Touch sono diversi e solo parzialmente compatibili (ad esempio, l'importazione di un backup di iPad in un iPhone non ripristinerà le foto);
- non è possibile scegliere il percorso di memorizzazione dei backup che sarà sempre lo stesso, ovvero *\Users\(username)\AppData\Roaming\Apple Computer\MobileSync\Backup* o *\Users\(username)\Apple\MobileSync\Backup* (per iTunes da *Microsoft Store*) su Windows e *~/Library/Application Support/MobileSync/Backup/* su Mac;
- per ogni dispositivo, iTunes memorizza e conserva un solo backup (a meno che l'utente non copi o sposti manualmente backup precedenti ad altri percorsi) in una cartella rinominata come stringa esadecimale a 40 caratteri corrispondente al codice identificativo UDID del dispositivo copiato.



I dati non memorizzati nel backup non cifrato di iTunes consistono essenzialmente nei seguenti:

- contenuti da iTunes e App Store o PDF scaricati direttamente su Apple Books;
- contenuti sincronizzati con iTunes, quali MP3s or CD, video, libri e foto;
- impostazioni di Face ID o Touch ID;
- dati relativi ad *Apple Pay;*
- dati relativi ad *Apple Mail;*
- dati relativi alle app *Activity*, *Health* and *Homekit* (inclusi nel backup cifrato);
- elenco chiamate;
- cronologia web e password *Safari;*
- dati del *Keychain* (inclusi nel backup cifrato).

Significativamente, i **dati classificati come sensibili**, ovvero quelli relativi alla salute (*Activity*, *Health*) e alla domotica (*Homekit*) non vengono memorizzati nei backup locali non protetti da password. Ai fini di un’acquisizione logica più completa, si rende quindi necessaria l’impostazione di una password di backup in modo da ottenere dati di maggior interesse investigativo quali, solitamente, la cronologia di navigazione e l’elenco delle chiamate. Si segnala che, in caso di backup non cifrati, viene comunque riportato l’elenco delle chiamate

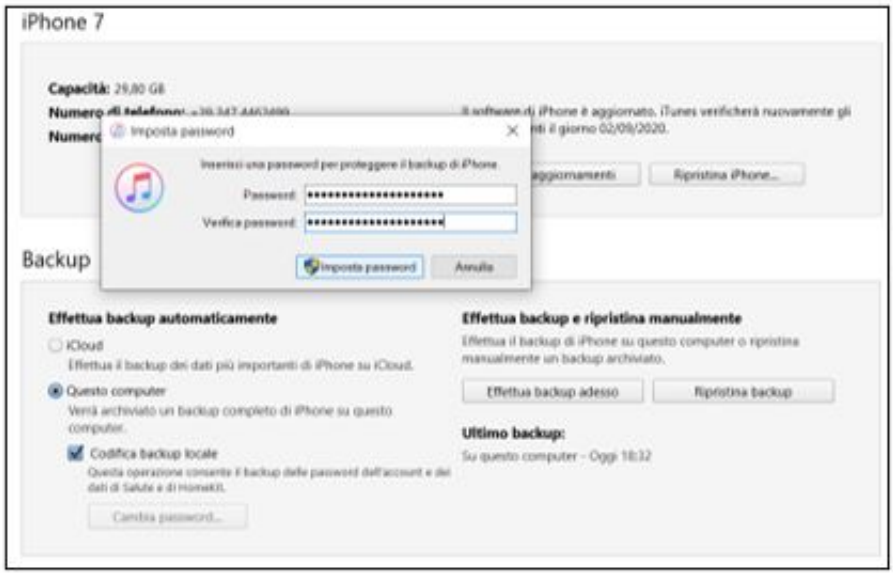
VoIP, omettendo solo le più tradizionali chiamate per via telefonica.
Similmente si ha per la cronologia di navigazione di *Safari* che, in caso di backup non cifrato, riporta comunque le ricerche web e i segnalibri ma non anche le pagine visitate dopo l'immissione degli URL o dei termini nei motori di ricerca e le password. Per gli altri browser web - quali Firefox o Chrome - la cronologia di navigazione è esportata per intero anche nel backup non cifrato, con l'eccezione delle password.

Una considerazione a parte merita il *Keychain*, ovvero il password manager di Apple utilizzato dal sistema operativo e dalle applicazioni per memorizzare password, token e certificati di sicurezza.

Tecnicamente il *Keychain* non omette di esportare il proprio contenuto nei backup privi di password, ma ne cifra i dati con una chiave memorizzata nel dispositivo che lo ha generato e non decifrabile da altri strumenti. In questo modo il backup del *Keychain* resta di fatto non importabile in dispositivi diversi e non analizzabile senza una previa estrazione della chiave di cifratura dal dispositivo che lo ha generato, tramite acquisizione fisica dello stesso. Il database SQL al percorso **/private/var/Keychains/keychain-2.db** che costituisce il *Keychain* non è tuttavia cifrato nella sua interezza, ma ne sono cifrati i record. A partire dagli iPhone 5S il sistema di gestione delle chiavi *hardware-based Secure Enclave* ne impedisce la decifratura al di fuori del dispositivo, aggiungendo un ulteriore livello di sicurezza.

iTunes encrypted backup

Nei backup iTunes protetti da password, l'intero contenuto del backup, incluso i dati del *Keychain*, viene cifrato con una chiave derivata dalla password scelta dall'utente.



In questo modo, i dati inclusi nel *Keychain* possono essere decifrati utilizzando l'apposita password ed eventualmente importati in un nuovo dispositivo, con l'**eccezione** degli oggetti per

cui è impostato l'attributo di sicurezza *ThisDeviceOnly*, i quali potranno essere ripristinati solo nel dispositivo che li ha generati. Apple concede infatti agli sviluppatori di poter scegliere questa misura come il livello più alto di protezione per i dati gestiti dalle applicazioni. In quest'ultimo caso, l'acquisizione fisica resta l'unica possibilità per la decifratura.

Segue nella seconda parte

Riferimenti

M. Epifani - P. Stirparo, *Learning iOS Forensics* – Packt Publishing
https://blog.elcomsoft.com/2014/03/itunes-icloud-backups/
https://blog.elcomsoft.com/2017/11/ios-11-horror-story-the-rise-and-fall-of-ios-security/
https://support.apple.com/en-ca/guide/security/aside/sec8e00e0dd8/1/web/1
https://support.apple.com/en-us/HT204136

Note

[1] https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-1-before-first-unlock.html

Articolo a cura di **Luca Cadonici**