iCloud Forensics

….e *privacy* dei nostri dati?

Milano, 21/6/2012

Convegno E-Privacy

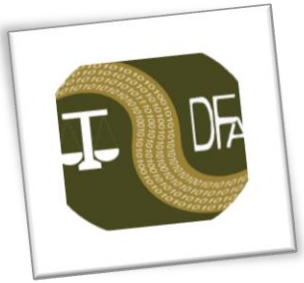
Mattia Epifani

Digital Forensics Alumni
Via Spallanzani, 16
20129 Milano
Fax.: +39 178 6071697

www.perfezionisti.it
info@perfezionisti.it

iCloud

- Il servizio ***iCloud***, introdotto da Apple nel giugno 2011, permette agli utenti di memorizzare i dati dai propri dispositivi su server remoti e condividerli
- Può essere utilizzato per fare il *backup* dei dispositivi Apple mobile (iPhone, iPad, iPod Touch)
- Può essere utilizzato per visualizzare online email, contatti, eventi, ecc.
- Permette di localizzare il dispositivo da remoto attraverso l'applicazione "Trova il mio dispositivo"
- Ad aprile 2012 contava circa **125 milioni di utenti**

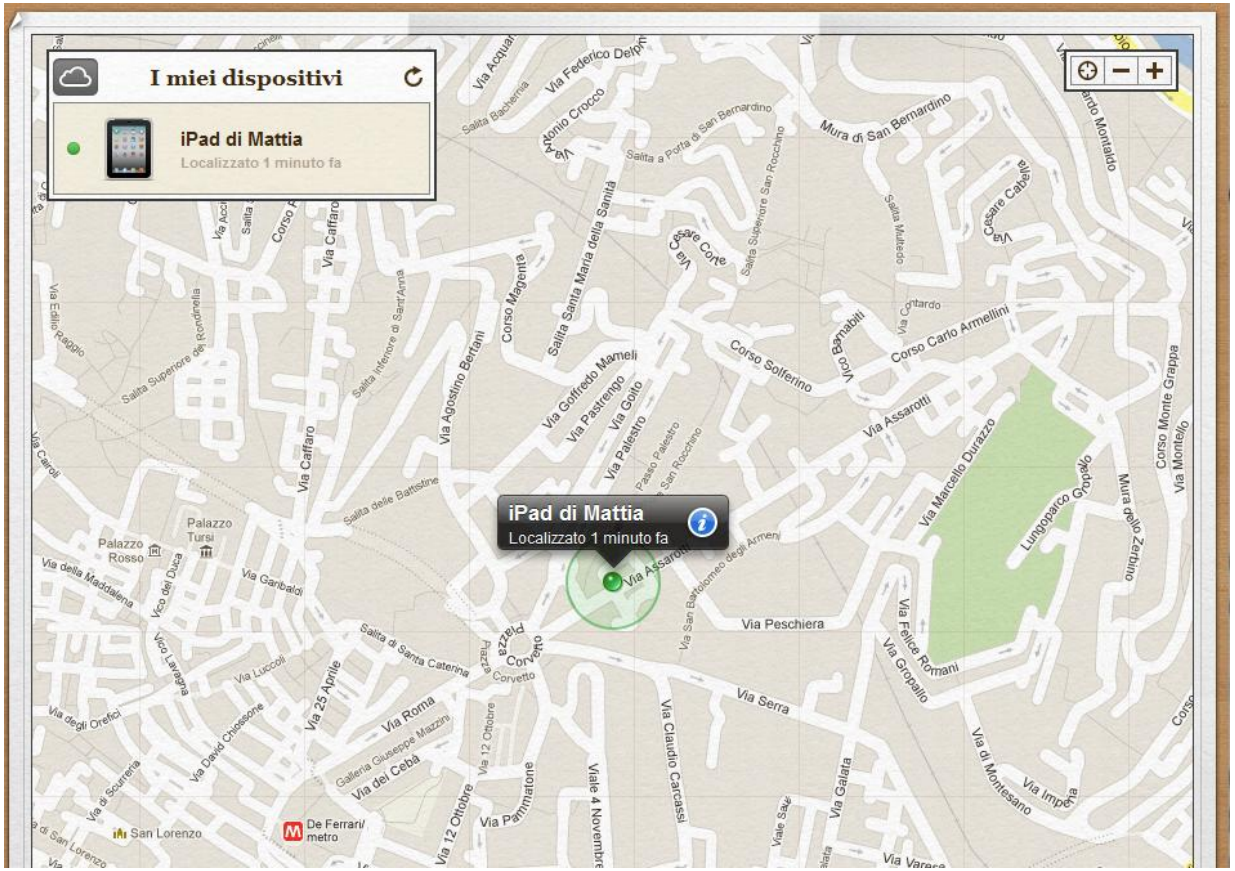


iCloud

iCloud


iCloud
Mattia Epifani
Esci
Mail
Contatti
domenica
3
Calendario
Trova il mio iPhone
iWork

iCloud


I miei dispositivi
iPad di Mattia
Localizzato 1 minuto fa
iPad di Mattia
Localizzato 1 minuto fa
Via Federico Delpino
Via Antonio Crocco
Salita a Porta di San Bernardino
Mura di San Bernardino
Via Caffaro
Corso Magenta
Salita Santa Maria della Sanità
Via Agostino Bertani
Via Goffredo Mameli
Via Pastrengo
Via Goito
Via Palestro
Corso Solferino
Corso Carlo Armellini
Via Assarotti
Via Marcello Durazzo
Lungoparco Gropallo
Mura dello Zerbino
Corso Monte Grappa
Via Montello
Salita delle Battistine
Palazzo Rosso
Palazzo Tursi
Via della Maddalena
Via Garibaldi
Via Luccoli
Via 25 Aprile
Via Roma
Via dei Ceba
Via 12 Ottobre
Via Pammatone
Viale 4 Novembre
Via Claudio Carcassi
Via Peschiera
Via Serra
Via Felice Romani
Via Gropallo
Via di Montesano
Via Galata
Via Imperia
Via Varese
San Lorenzo
De Ferrari/ metro

iCloud


Info
iPad di Mattia
Localizzato 1 minuto fa
Emetti un suono o invia un messaggio
Blocco remoto
Cancell. remota

iCloud

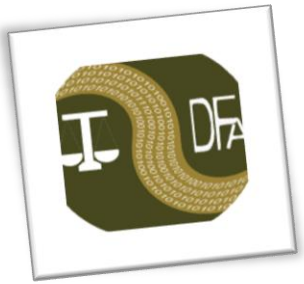

Annulla
Blocco remoto
Blocca
Inserisci un codice.
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

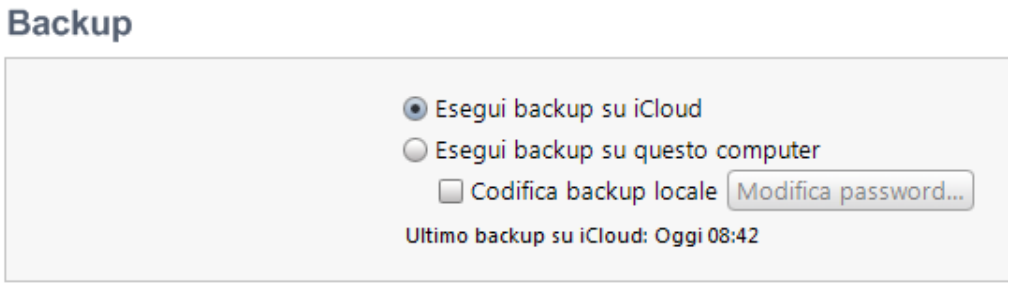
iCloud


Info
Questa operazione cancellerà tutti i dati e non può essere annullata. Non è possibile individuare un iPad se i suoi dati sono stati cancellati in remoto.
Se ritrovi il tuo iPad, alcuni servizi potrebbero essere temporaneamente non disponibili dopo il ripristino.
Cancella i dati
Annulla

iCloud Backup

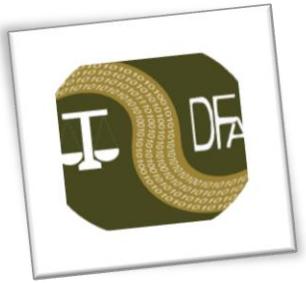
- I *backup* online di *iCloud* sono **incrementali** (mediante ***snapshot***)
- Una volta attivato il servizio, il dispositivo effettua automaticamente il *backup* ogni volta che:
  - E' connesso alla corrente elettrica
  - E' collegato ad una rete WiFi
  - Ha lo schermo bloccato
- Ogni *snapshot* rappresenta quindi lo stato attuale del dispositivo al momento della sua creazione





iCloud Backup

- Un *backup* può contenere, tra gli altri:
  - Messaggi (*iMessage*, *SMS*, *MMS*)
  - Email
  - Immagini e video acquisiti dalla fotocamera
  - Calendari
  - Contatti
  - Formato file PDF salvati in *iBook* (es. libri acquistati, allegati da mail salvati, ecc.)
  - Cronologia di navigazione
  - Dati e impostazioni delle applicazioni….



iCloud Backup

- ***iCloud: Backup and restore overview***

  http://support.apple.com/kb/HT4859

What is backed up

You get unlimited free storage for:

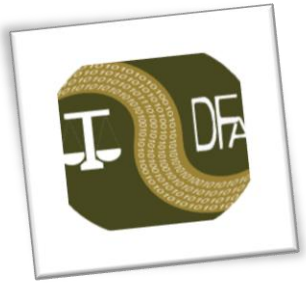
- Purchased music, movies, TV shows, apps, and books

  Notes: Backup of purchased music is not available in all countries. Backups of purchased movies and TV shows are U.S. only. Previous purchases may not be restored if they are no longer in the iTunes Store, App Store, or iBookstore.

  Some previously purchased movies may not be available in iTunes in the Cloud. These movies will indicate that they are not available in iTunes in the Cloud on their product details page in the iTunes Store. Previous purchases may be unavailable if they have been refunded or are no longer available in the iTunes Store, App Store, or iBookstore.

You get 5GB of free iCloud storage for:

- Photos and videos in the Camera Roll
- Device settings (for example: Phone Favorites, Wallpaper, and Mail, Contacts, Calendar accounts)
- App data
- Home screen and app organization
- Messages (iMessage, SMS, and MMS)
- Ringtones



iCloud Backup

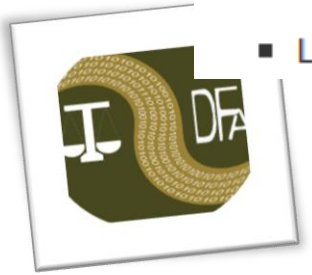
iCloud Backup

- ***iCloud: iCloud security and privacy overview***
  http://support.apple.com/kb/HT4865

Encrypting content that is stored in iCloud

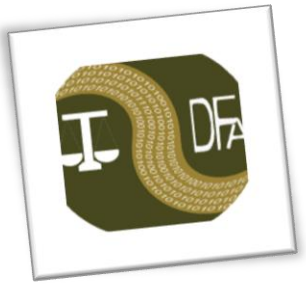
Apple encrypts data that is stored to deliver the iCloud service. Encrypted data includes:

- Photos in your Photo Stream
- Documents in the Cloud
- Backup data for your iOS device
- Contacts
- Calendars
- Bookmarks
- Reminders
- Location data for Find My iPhone, iPad, iPod touch, and Mac
- Location data for Find My Friends



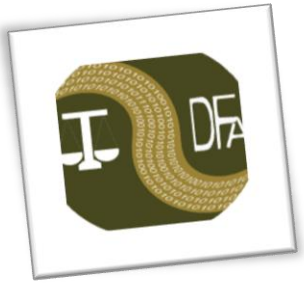
iCloud Backup

- I backup effettuati online sono a tutti gli effetti **non cifrati**
- Tecnicamente sono cifrati ma **la chiave di cifratura è memorizzata insieme ai file cifrati**
- Questa scelta è per consentire il ripristino del backup su un dispositivo diverso da quello che lo ha generato
- Le uniche informazioni necessarie quindi per accedere a un backup memorizzato su iCloud sono **le credenziali dell'utente**

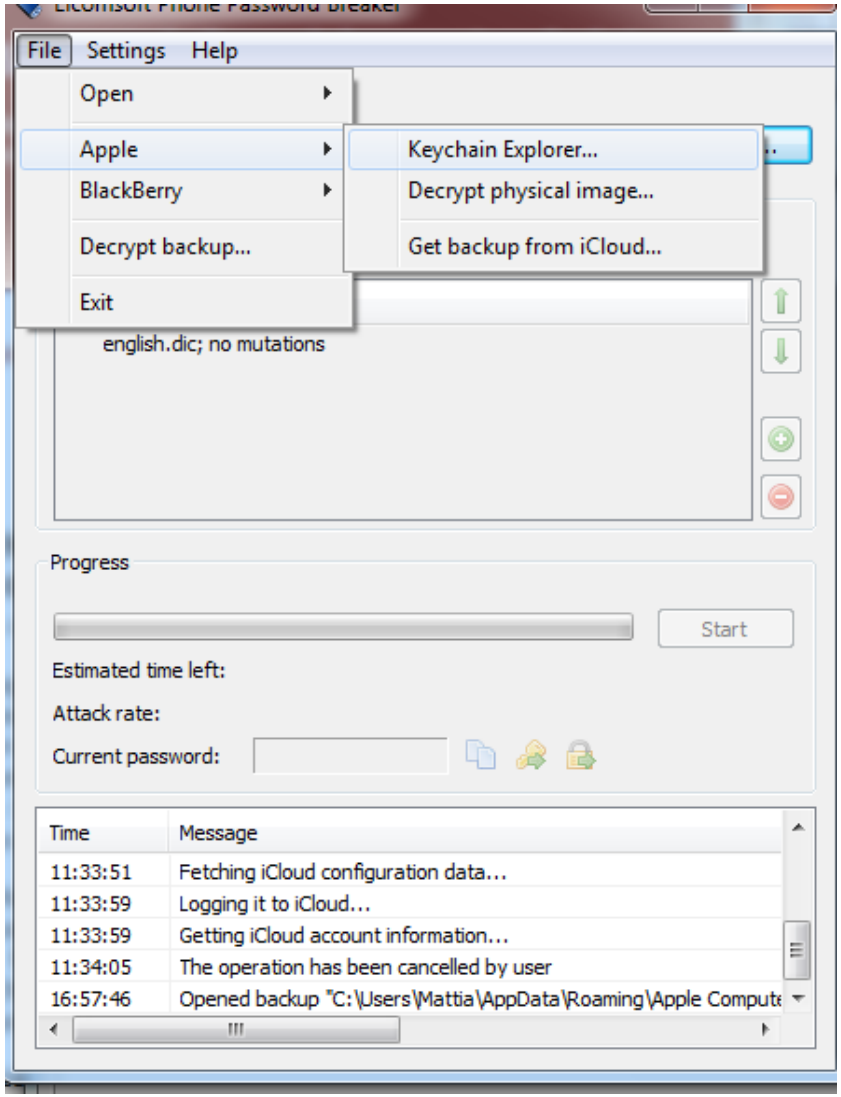


Dove trovo le credenziali?

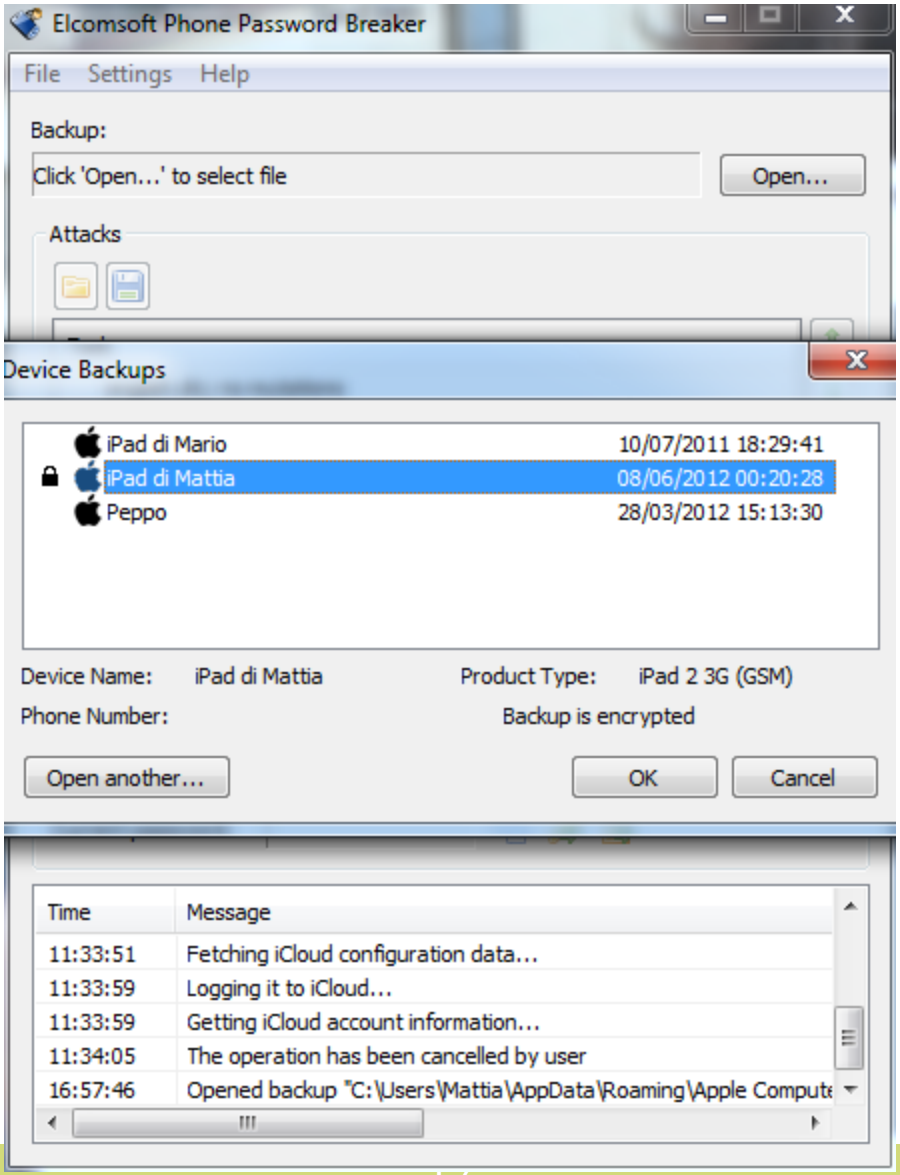
- Le credenziali di accesso a iCloud possono essere recuperate:
  - Mediante *Social Engineering* ☺
  - Da un PC o MAC su cui sia memorizzata
    - *iTunes Password Decryptor* (http://securityxploded.com/)
    - *Web Browser Pass View* (http://www.nirsoft.net/)
  - Direttamente dal dispositivo (iPhone, iPad, iPod Touch)
    - Se non è bloccato da *passcode* → E' sufficiente fare un *backup* cifrato con una *password* nota e il file keychain viene cifrato con tale *password*
    - Se è bloccato da *passcode* → Acquisizione completa del dispositivo e *bruteforce* del *passcode* (diverse soluzioni disponibili)



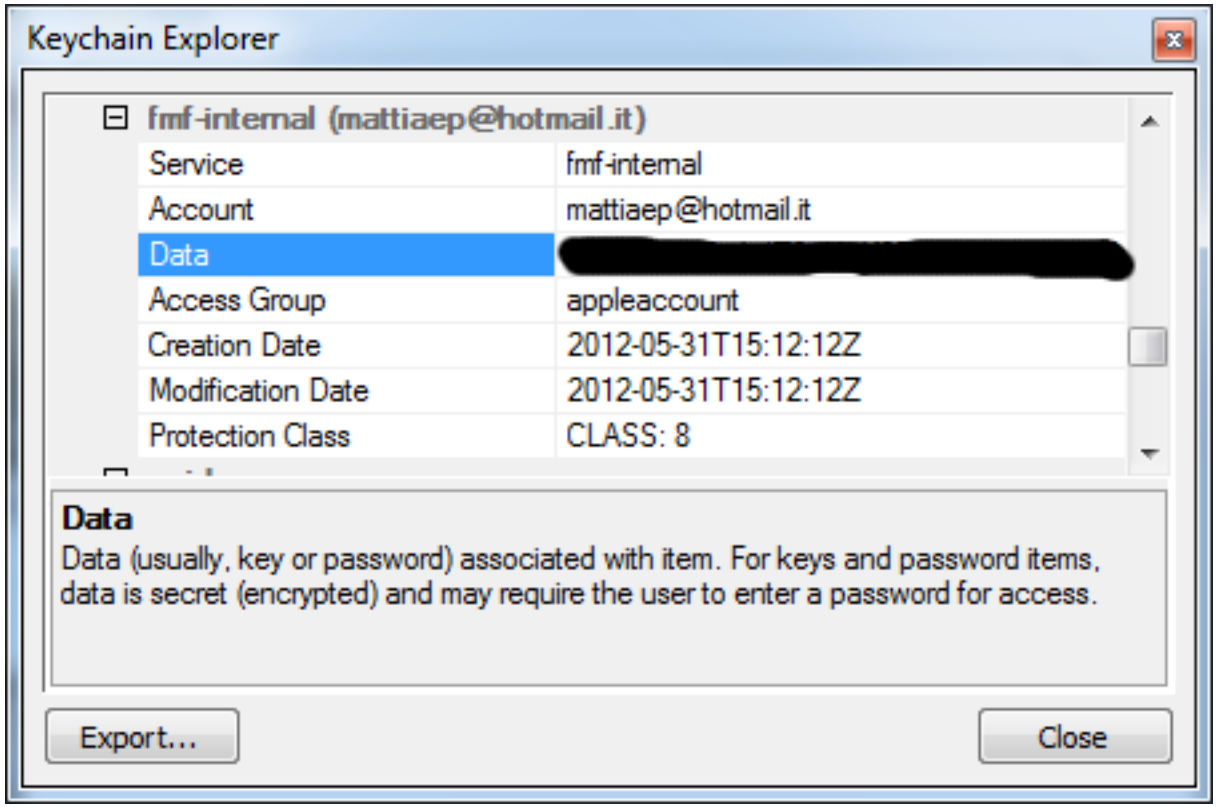
Phone Password Breaker



Phone Password Breaker



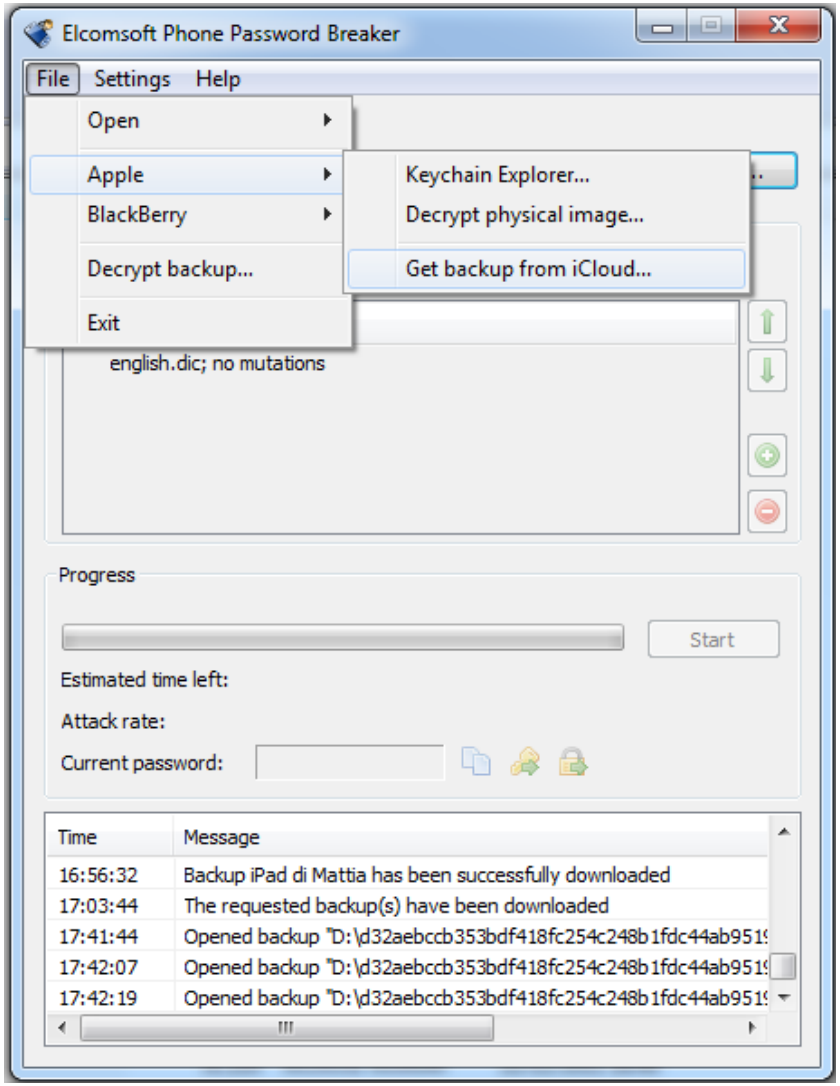
Phone Password Breaker



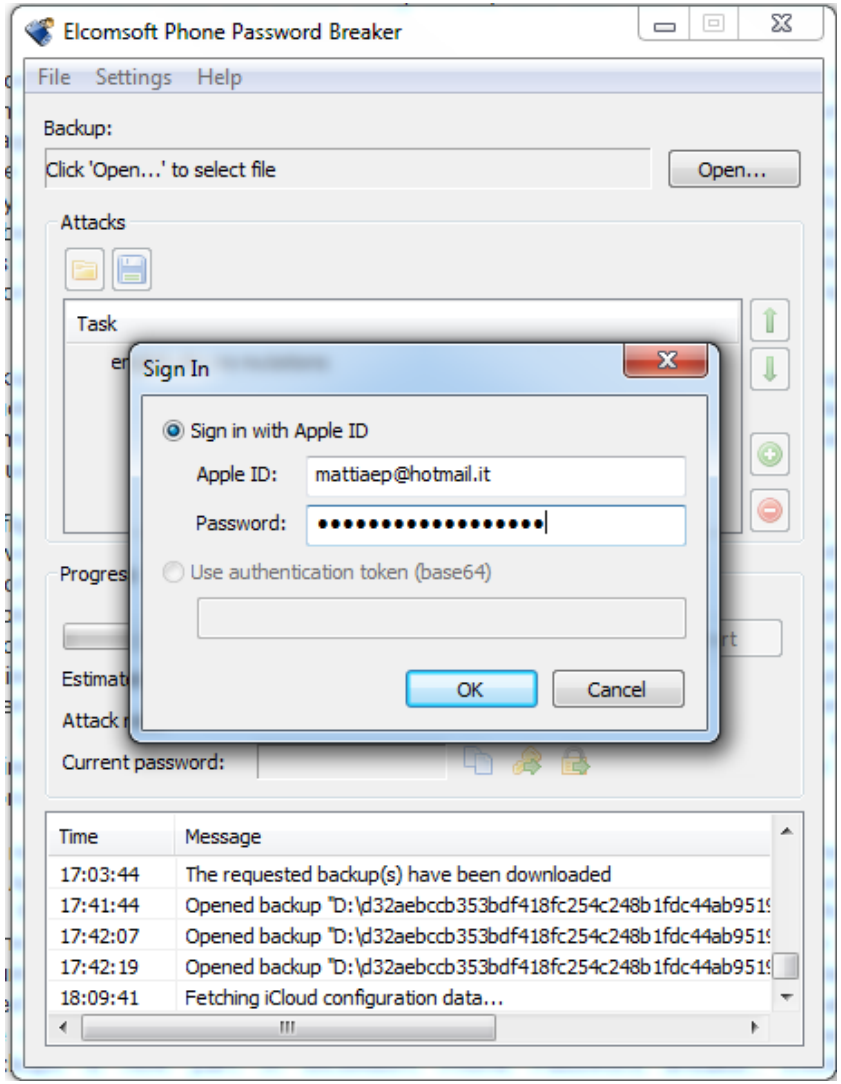
iCloud Backup

- I ricercatori della software house russa Elcomsoft hanno analizzato il protocollo di comunicazione tra *iDevice* e *Apple iCloud* e sono riusciti ad emulare i corretti comandi per recuperare il contenuto dello *storage iCloud* di un utente
- I dati sono ricevuti **direttamente in chiaro** (ovvero decifrati al volo) e possono essere salvati sul computer di chi sta effettuando l'acquisizione
- Le operazioni di download sono completamente trasparenti all'utente proprietario del dispositivo ed è quindi possibile "tenere sotto controllo" le attività dell'utente stesso…

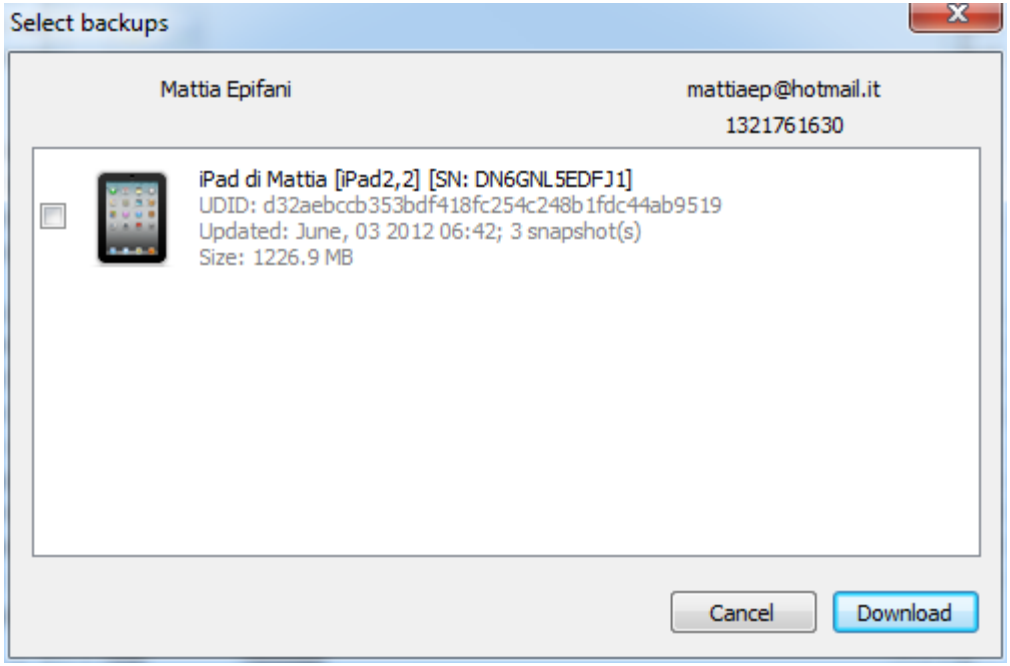
Phone Password Breaker



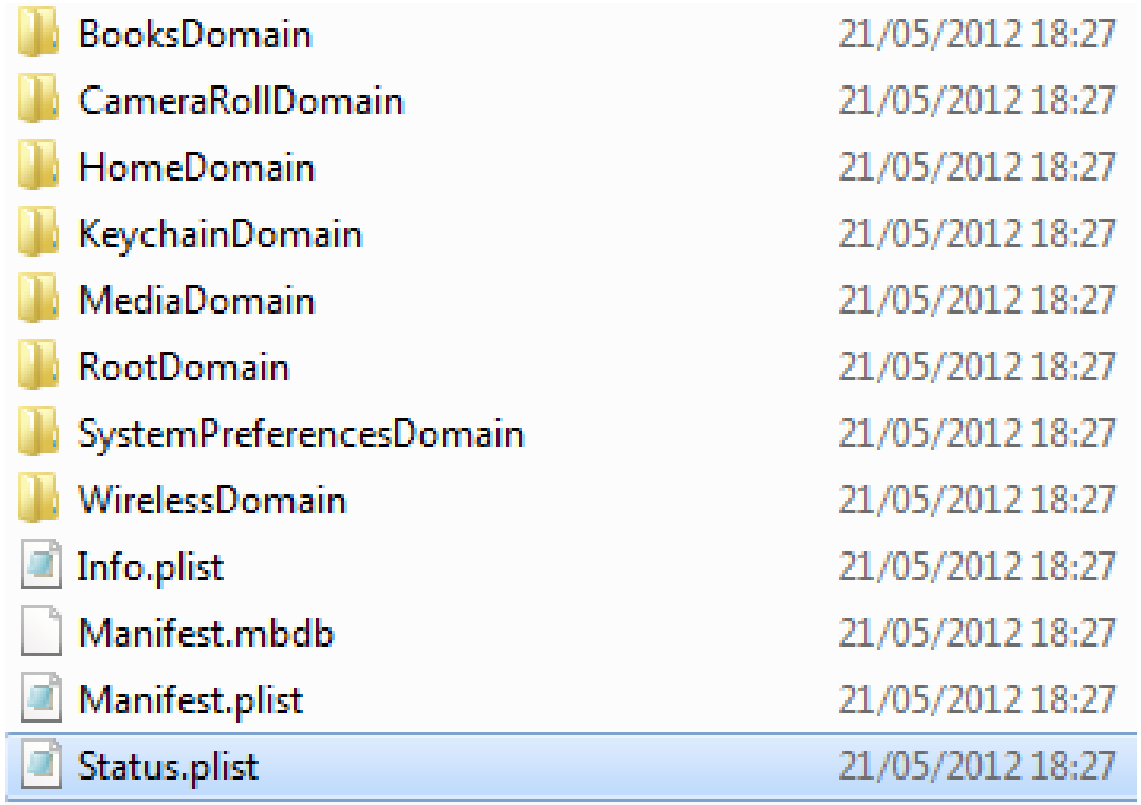
Phone Password Breaker



Phone Password Breaker



Struttura dei file



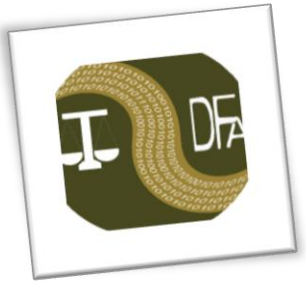
iCloud Forensics

- L'installazione del servizio *iCloud* su un PC lascia diverse tracce
- Log delle azioni sul PC

  C:\Users\<*nomeutente*>\AppData\Roaming\Apple Computer\Logs
- Impostazioni specifiche per l'utente

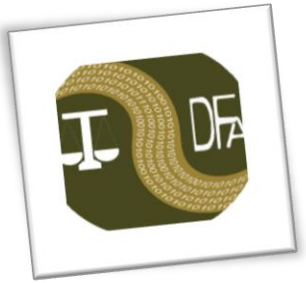
  C:\Users\<*nomeutente*>\AppData\Roaming\Apple Computer\Preferences
  - **mobilemeaccounts.plist**: nome dell'utente utilizzato
- Per approfondimenti

  http://forensicartifacts.com/2012/02/icloud-service-on-windows/



Conclusioni

- Se un utente malintenzionato scopre le credenziali di accesso ad *iCloud* ha la possibilità da remoto di:
  - Bloccare il dispositivo dell'utente attivando un codice di protezione
  - Cancellare il contenuto del dispositivo
  - Localizzare l'utente in tempo reale
  - Tenere sotto controllo le azioni e i dati dell'utente scaricando i diversi "*snapshot*"
- Se un utente dismette un dispositivo e non elimina l'account su *iCloud* il *backup* rimane su *iCloud*…




CLOUD COMPUTING
PROTEGGERE I DATI
PER NON CADERE DALLE NUVOLE
Mini guida per imprese
e pubblica amministrazione
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Grazie per l’attenzione

mattia.epifani@digital-forensics.it