HACK IN BO®
Spring 2023 Edition
20ª EDIZIONE

Freezing Internet Tool

FABIO ZITO

FRANCESCA POLLICELLI

Chi sono

(@ZiteLOG)

Alcune premesse prima di iniziare

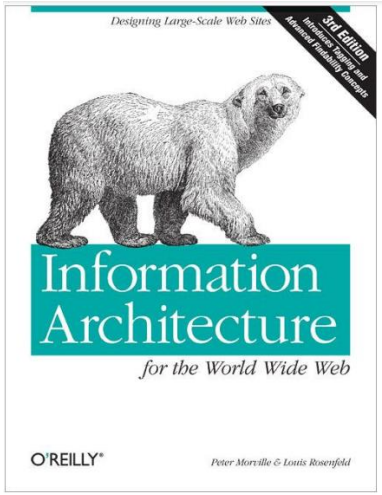
Che cos’è la Digital Forensics?

In generale, le procedure di *Digital Forensics* definiscono **le modalità di identificazione**, **acquisizione e analisi di una prova digitale, preservando lo stato originale della stessa (INTEGRITÀ E AUTENTICITÀ) al fine di poter essere presentata in un procedimento giuridico***.

**“*Dal punto di vista giuridico, tali procedure sono regolate dalla legge 48 del 2008 nella quale il legislatore ha recepito quanto previsto nella Convenzione di Budapest del 2001, ossia, che l’attività di acquisizione sia effettuata “adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione” Detta legge, inoltre, ha introdotto il comma 1bis all’art. 247 nel codice di procedura penale, che recita esattamente lo stesso principio.*

Cosa intendiamo per contenuto web

qualunque elemento che possa essere incluso all'interno di un documento HTML.



**"We define content broadly as 'the stuff in your Web site.' This may include documents, data, applications, e-services, images, audio and video files, personal Web pages, archived e-mail messages, and more. And we include future stuff as well as present stuff."*

Acquisire un contenuto WEB è più complesso rispetto ad altri?

Probabilmente SI:

1. E’ difficile accedere “fisicamente” al server sul quale il contenuto è memorizzato

2. Il contenuto stesso ha alcune peculiarità che lo rendono differente da altri contenuti digitali

Informazioni facilmente deperibili

Le informazioni presenti sul web sono soggette a continua trasformazione e la velocità con cui avvengono determinati cambiamenti rende, di fatto, tali informazioni facilmente deperibili.

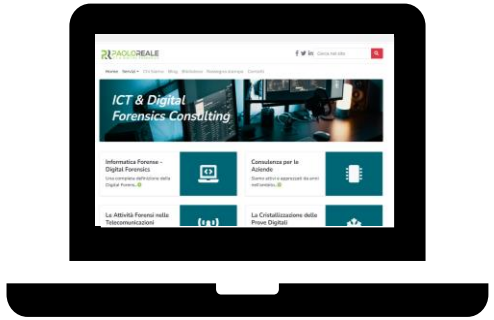
I contenuti si possono presentare in modo diverso

in base al tipo di **monitor,**

alla sua **localizzazione**,

alla **connettività**, etc…

Da PC



Da Smartphone

Gli elementi invisibili

Cioè quegli elementi che sono parte della pagina, ne influiscono il comportamento, ma non sono «visibili».

Uno *screenshot* non è sufficiente

Non è sufficiente uno *screenshot* per cristallizzare un contenuto web.

- **Evidenza non attendibile:** potrebbe essere realizzato ad hoc con un qualsiasi strumento di grafica e, in più, sarebbe privo di tutte quelle componenti non visibili a schermo (JAVASCRIPT, CSS, HTML, etc.) che sono parte del contenuto stesso.

- **Devono essere acquisiti a "corredo" altri elementi** quali, ad esempio, il video delle operazioni svolte, la registrazione del traffico di rete, il calcolo delle hash, etc.

Nel passato…

per bypassare «**il problema dello *screenshot*»** veniva fatta una “copia conforme” (art. 2712 c.c.) dell’immagine della pagina WEB certificata da un Notaio, ma anche un Notaio può certificare solo quello che vede sul monitor del proprio PC.

Quale sarà quello falso?

Quindi cosa bisogna acquisire?

- **Codice sorgente** della pagina e di tutti gli elementi che la compongono (HTML, CSS, JS, immagini,…)
- **Log con la registrazione** di tutte le operazioni effettuate con relativa video registrazione
- **Screenshot** del sito
- **Registrazione** del traffico di rete
- **Hash** di ogni elemento acquisito

Cos’è FIT?

- **Genesi**: Applicazione sviluppata in Python (3) per l'acquisizione forense di contenuti web. Realizzata inzialmente da Fabio Zito come tesi di Master, che da inizio 2023 si è trasformata nel progetto FIT.

- **Tool sviluppato da informatici forensi per informatici forensi:** grazie alla partecipazione attiva degli esperti **ONIF** (Osservatorio Nazionale Informatica Forense).

- **Qualche info tecnica:** Architettura modulare, Pattern MVC. Disponibile su https://github.com/fit-project/fit attualmente sono state scritte circa **7K righe di codice** e sono stati fatti **più di 500 commit.**

I plus di FIT

MULTIPIATTAFORMA*	MODULARE	OPENSOURCE	FATTO DA INF. FORENSI	ANTI-TAMPERING
Win, Lin, Mac	Facilmente Ampliabile	Community di sviluppo e test	Per informatici forensi	Maggiore Sicurezza

*Attualmente solo per windows

HACK IN BO®
Spring 2023 Edition
20ª EDIZIONE

Cosa fa **FIT**?

Chi sono

Laurea Magistrale in Sicurezza Informatica (progetto FIT)

Laurea Triennale in Informatica e Tecnologie per la Produzione del Software (sistemi biometrici e crittografia)

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

@fpollicelli

@frapple#1605

Acquisizione web

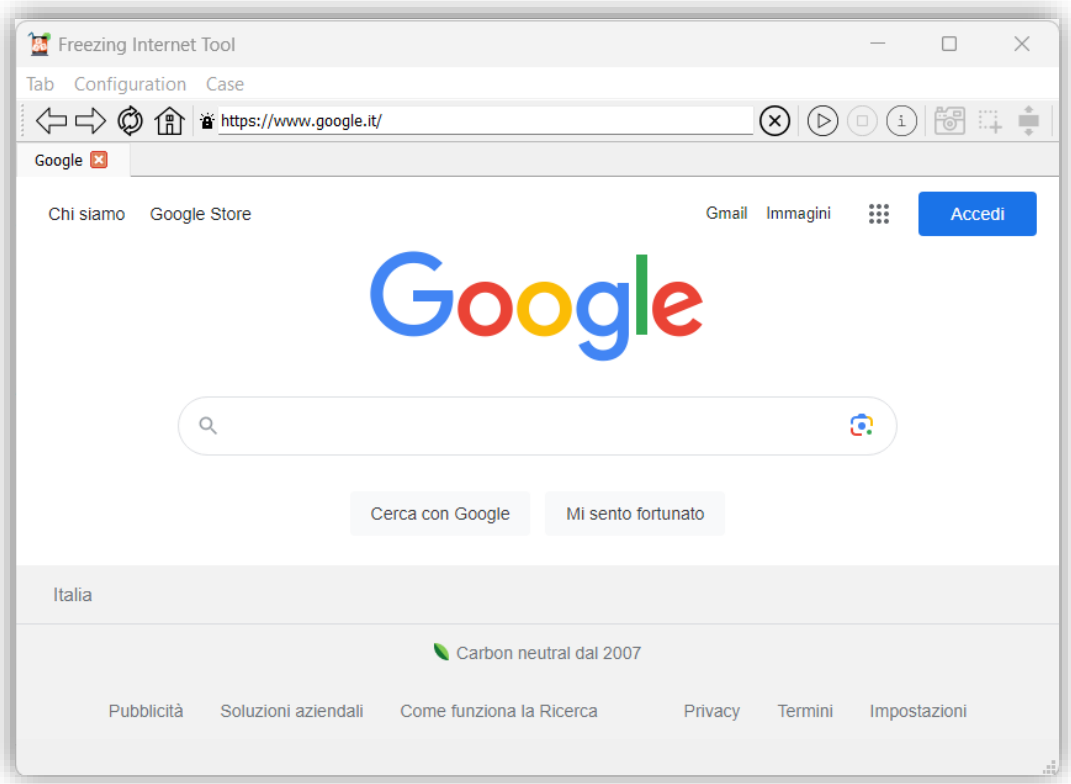
Il tool di acquisizione web consente la cristallizzazione delle pagine.

Cosa acquisisce?

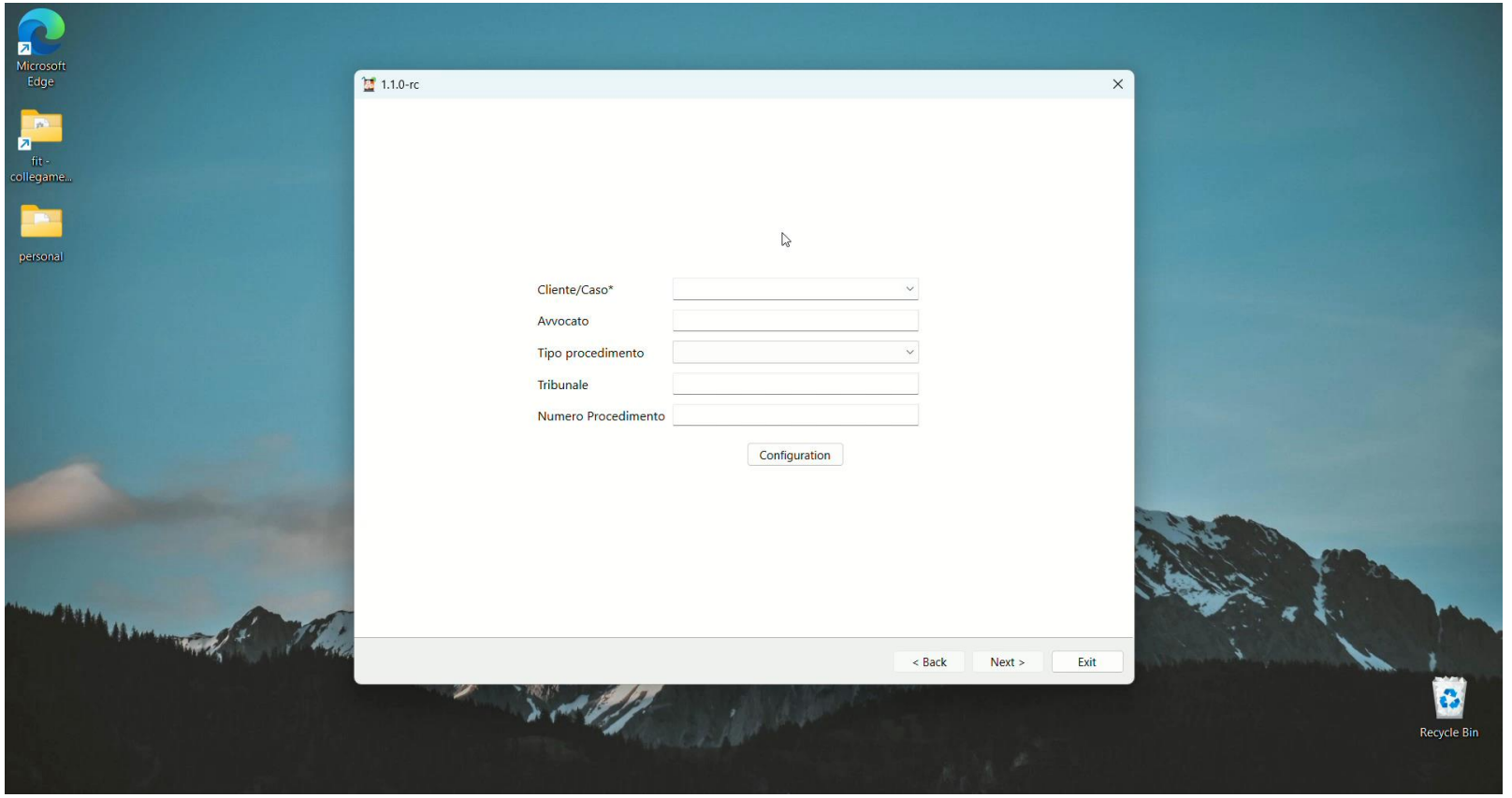
Codice HTML, fogli di stile, JavaScript, immagini.

Inoltre…

Screenshot multipli della pagina consultata, registrazione video dell'acquisizione, log delle operazioni, cattura dei pacchetti, headers, chiavi SSL, whois, nslookup, certificato del server, triplo hash di ogni elemento.



FIT in azione: acquisizione web



Acquisizione Instagram

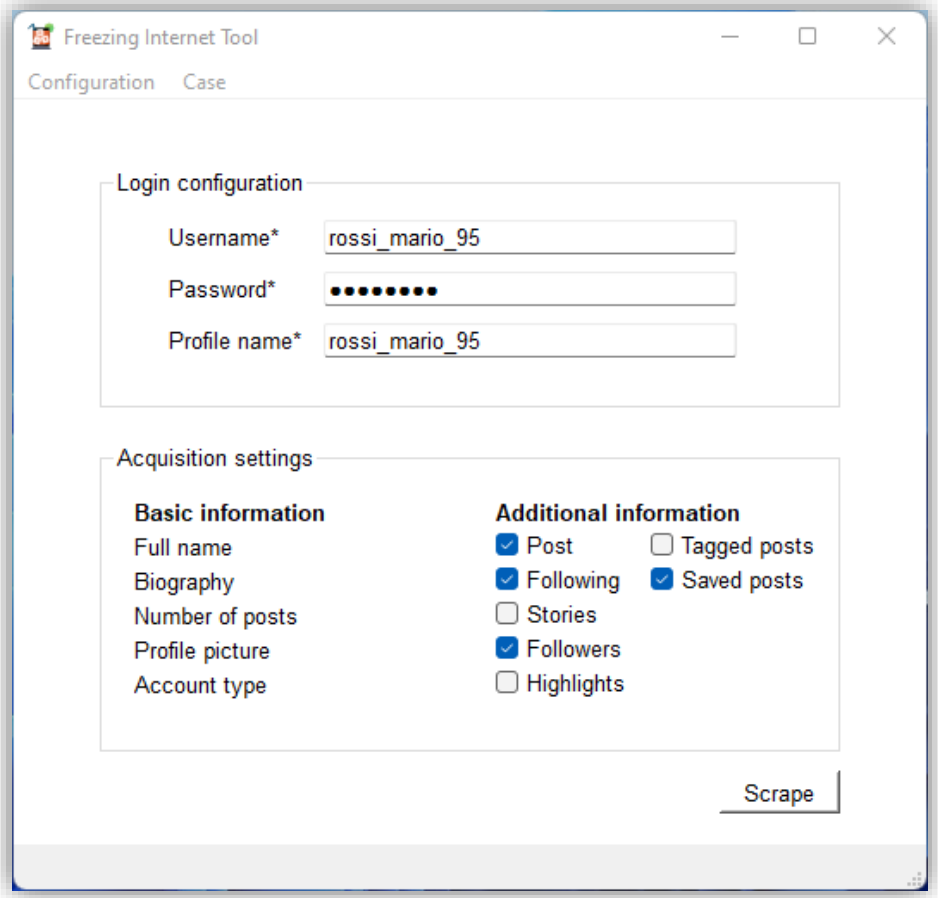
Il tool di acquisizione Instagram consente la cristallizzazione dei profili.

Cosa acquisisce?

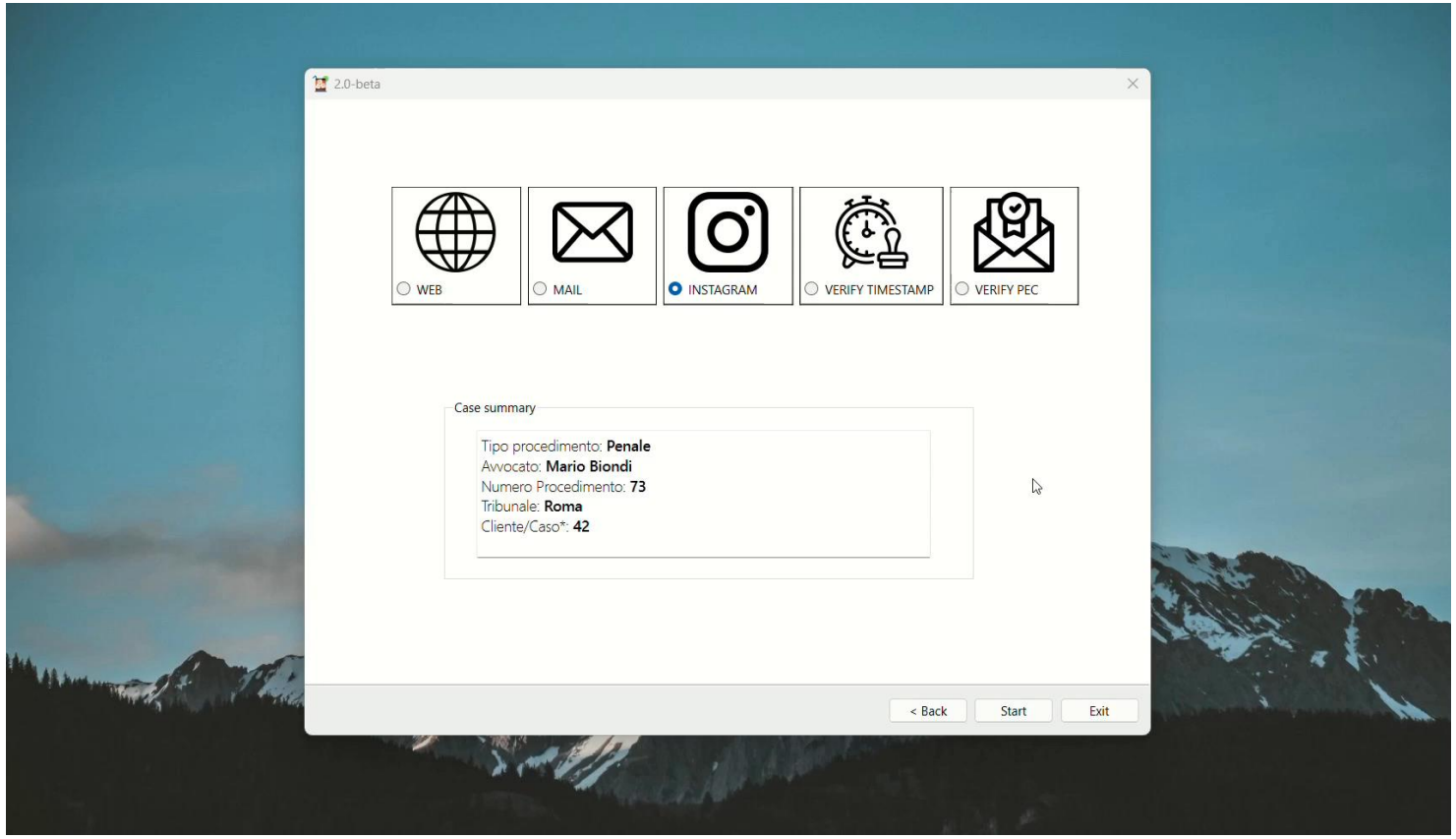
Nome dell'account, biografia, numero di post, immagine del profilo, tipo di account, post, utenti seguiti, utenti seguaci, storie, storie in evidenza, post taggati, post salvati.

Inoltre…

Log delle operazioni, triplo hash di ogni elemento.



FIT in azione: acquisizione Instagram



Acquisizione e-mail

Il tool di acquisizione e-mail consente la cristallizzazione delle caselle di posta.

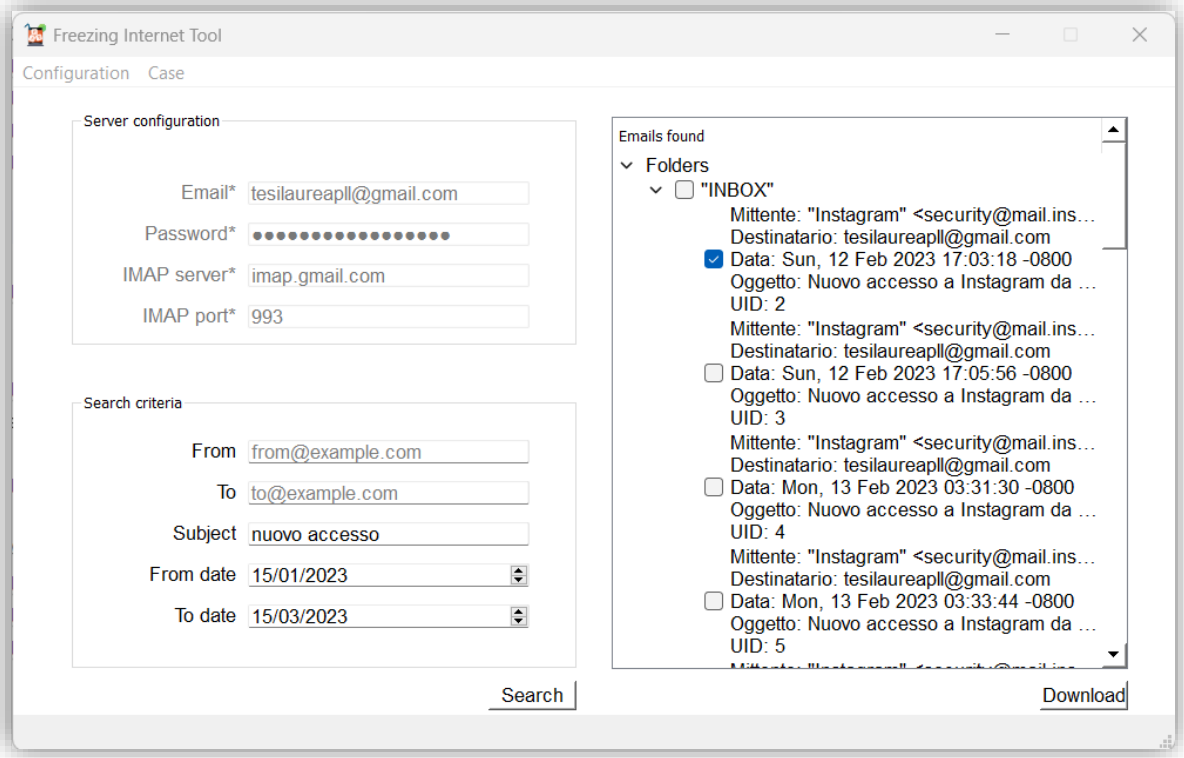
Cosa acquisisce?

E-mail complete di allegati in formato .eml da qualsiasi cartella (in arrivo, inviate, cestino, spam…).

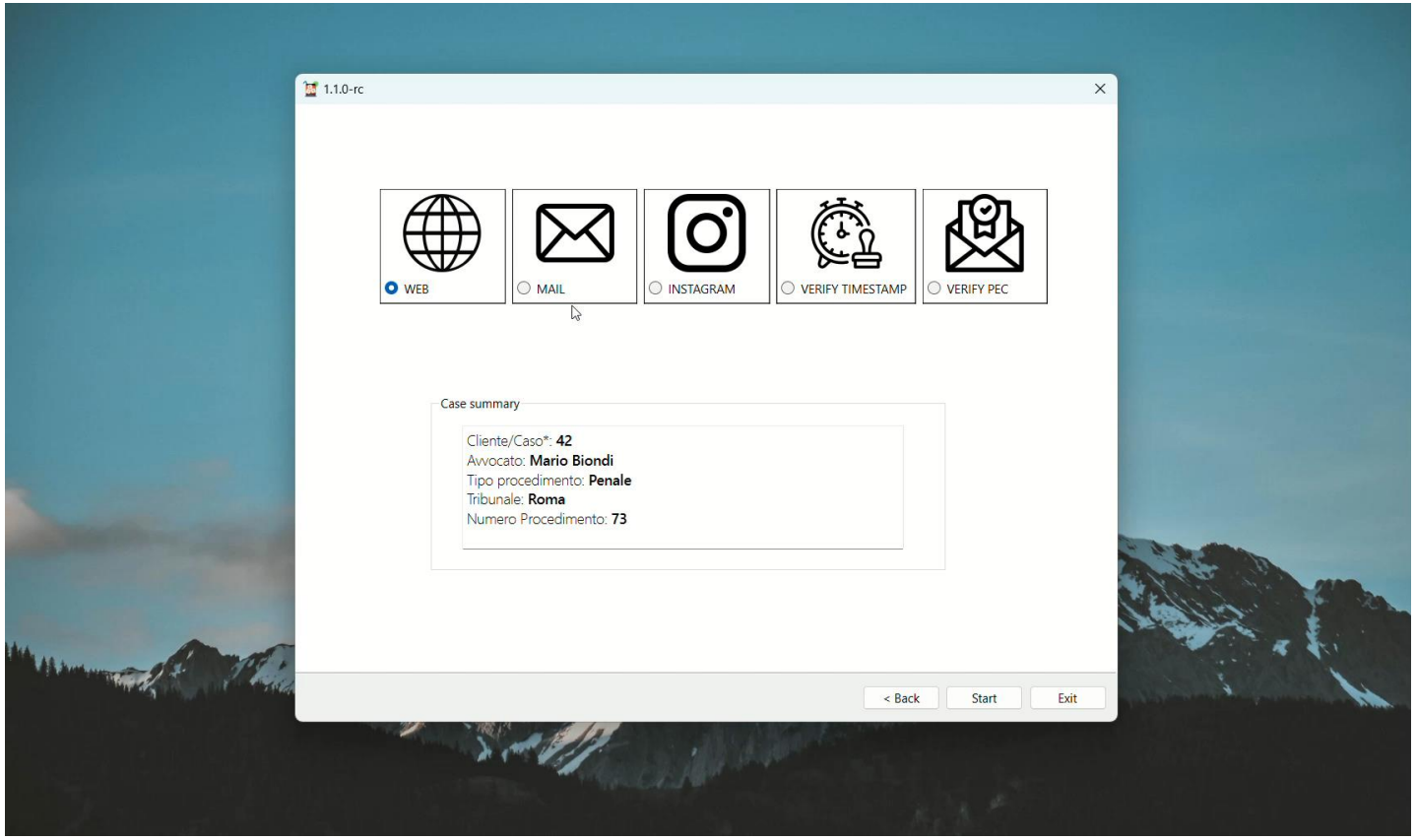
È possibile applicare filtri di ricerca e scegliere le e-mail da scaricare.

Inoltre…

Log delle operazioni, triplo hash di ogni elemento.



FIT in azione: acquisizione e-mail



Bello, ma come proteggiamo le informazioni?

La manomissione delle prove

La manomissione delle prove si riferisce a situazioni in cui una prova viene alterata, falsifica oppure occultata.

La manomissione potrebbe avvenire anche dopo che le informazioni sono state acquisite.

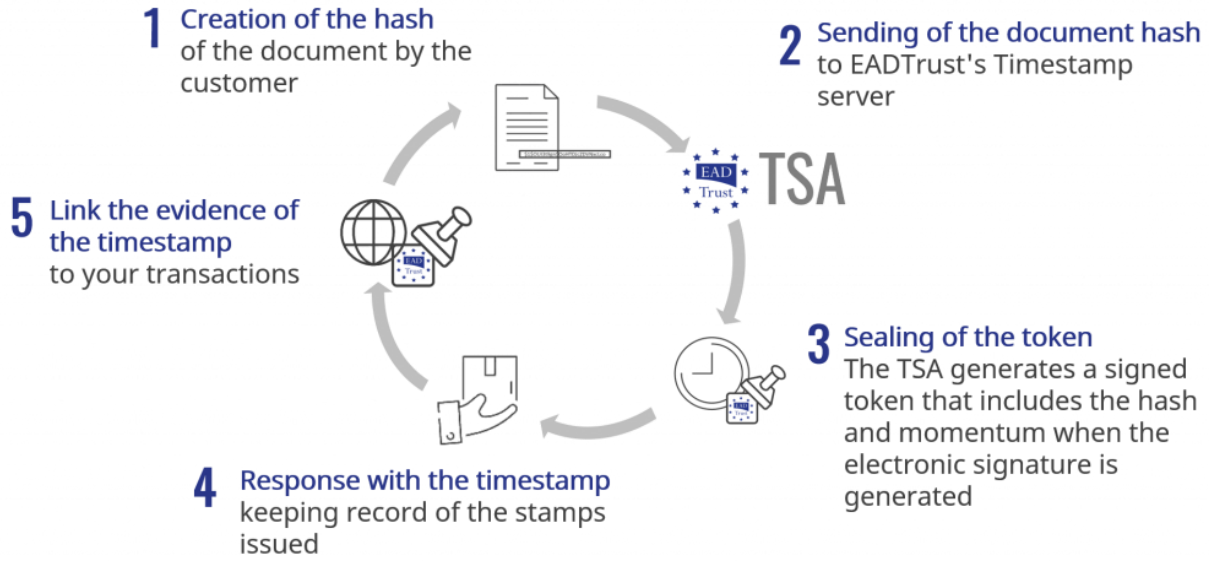
Esempio: dopo aver scaricato una e-mail, viene generato il file contenente i digest. Se modifichiamo l'e-mail e ricalcoliamo gli hash, la modifica non potrà essere rilevata in alcun modo.

È possibile adoperare delle tecniche di **anti-tampering:** garantiscono l'integrità delle informazioni prevenendo i tentativo di alterazione dei dati da parte di terzi.

Quali tecniche?

Oltre al calcolo degli hash…

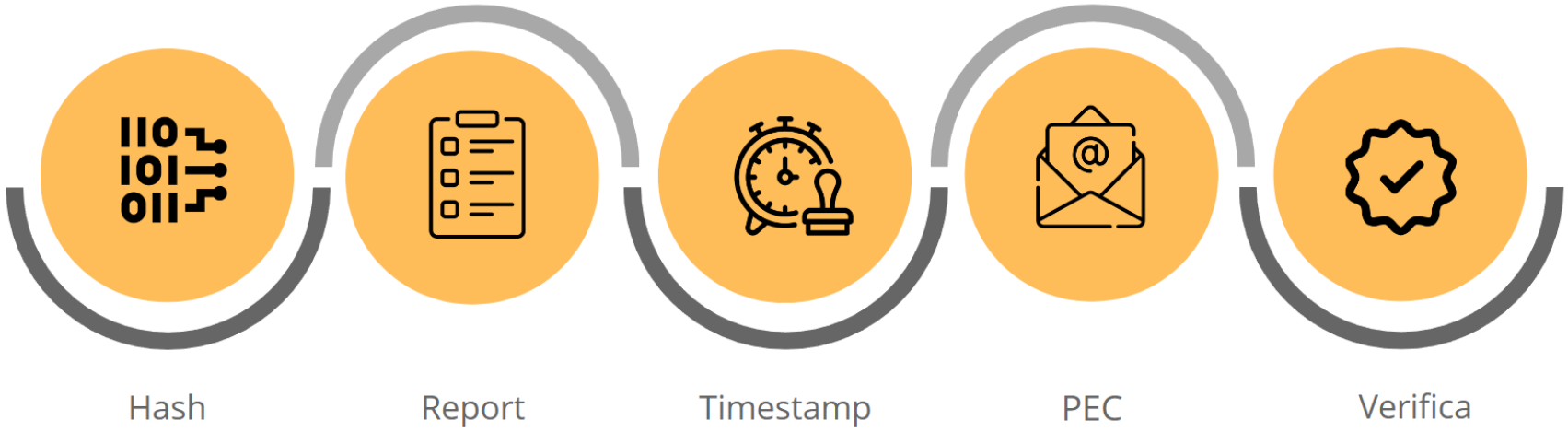
- **Timestamp** certificato, il quale garantisce l'integrità del dato, nonché ora e data di creazione
- Inoltro delle evidenze a soggetti autorizzati (ad esempio utilizzando la **PEC**)
- **Archiviazione sicura** tramite conservazione sostitutiva



Quale usiamo?

Una combinazione!

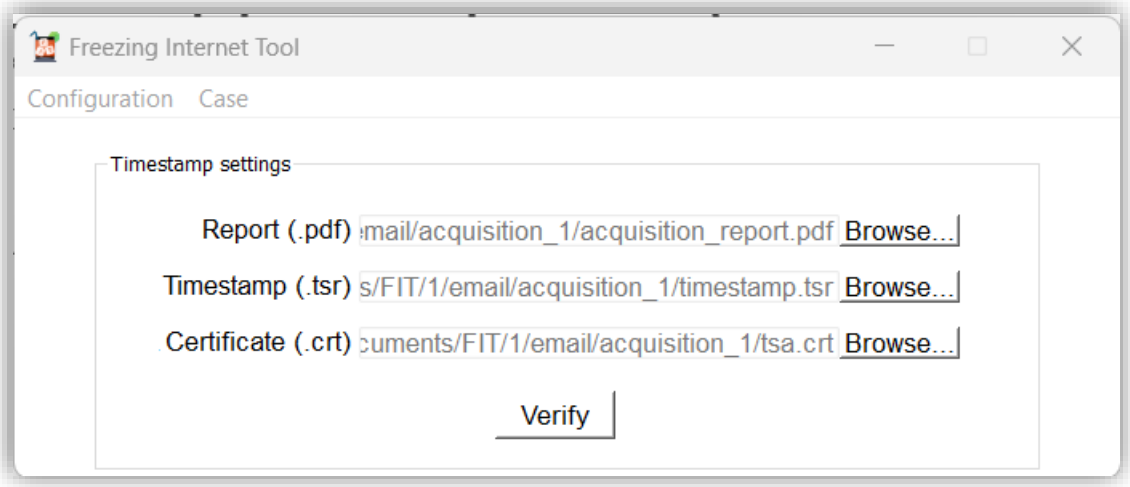
- FIT calcola il triplo **hash** di ogni elemento, inserisce tutti gli hash in un **report**, crea un **timestamp** certificato del report e invia report e timestamp tramite **PEC**.
- Inoltre, consente di **verificare** sia la validità del timestamp che il certificato della PEC.

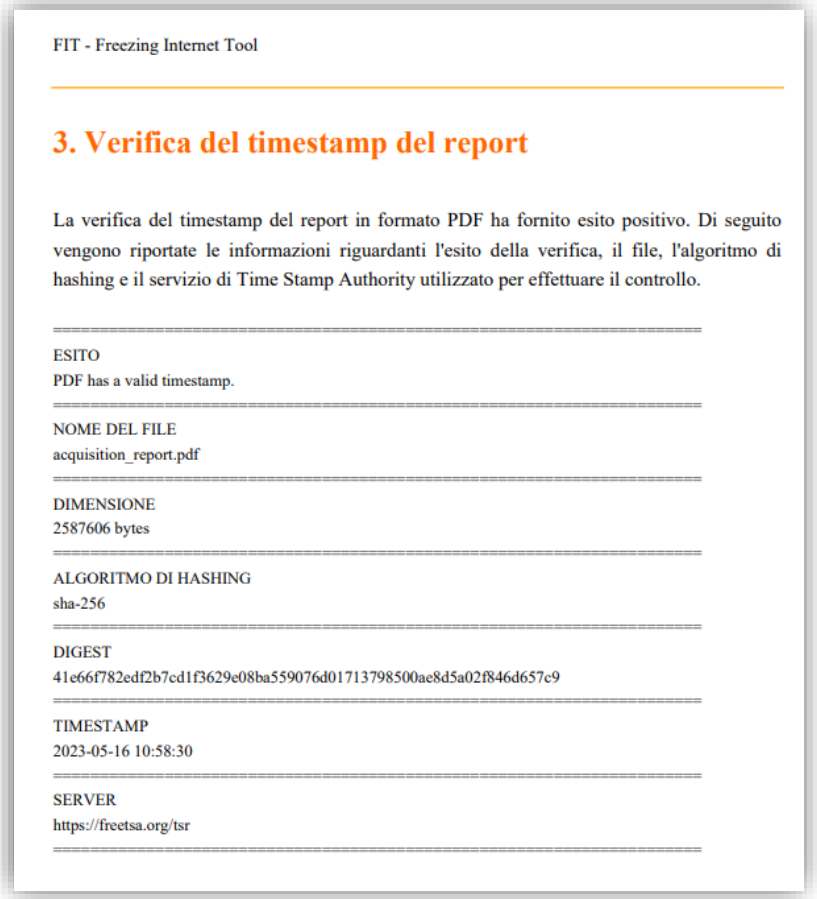


Come verifico il timestamp?

Con un tool integrato!

Il tool genera un report di verifica contenente tutte le informazioni riguardanti il timestamp.





FIT - Freezing Internet Tool

3. Verifica del timestamp del report

La verifica del timestamp del report in formato PDF ha fornito esito positivo. Di seguito vengono riportate le informazioni riguardanti l'esito della verifica, il file, l'algoritmo di hashing e il servizio di Time Stamp Authority utilizzato per effettuare il controllo.

ESITO
PDF has a valid timestamp.

NOME DEL FILE
acquisition_report.pdf

DIMENSIONE
2587606 bytes

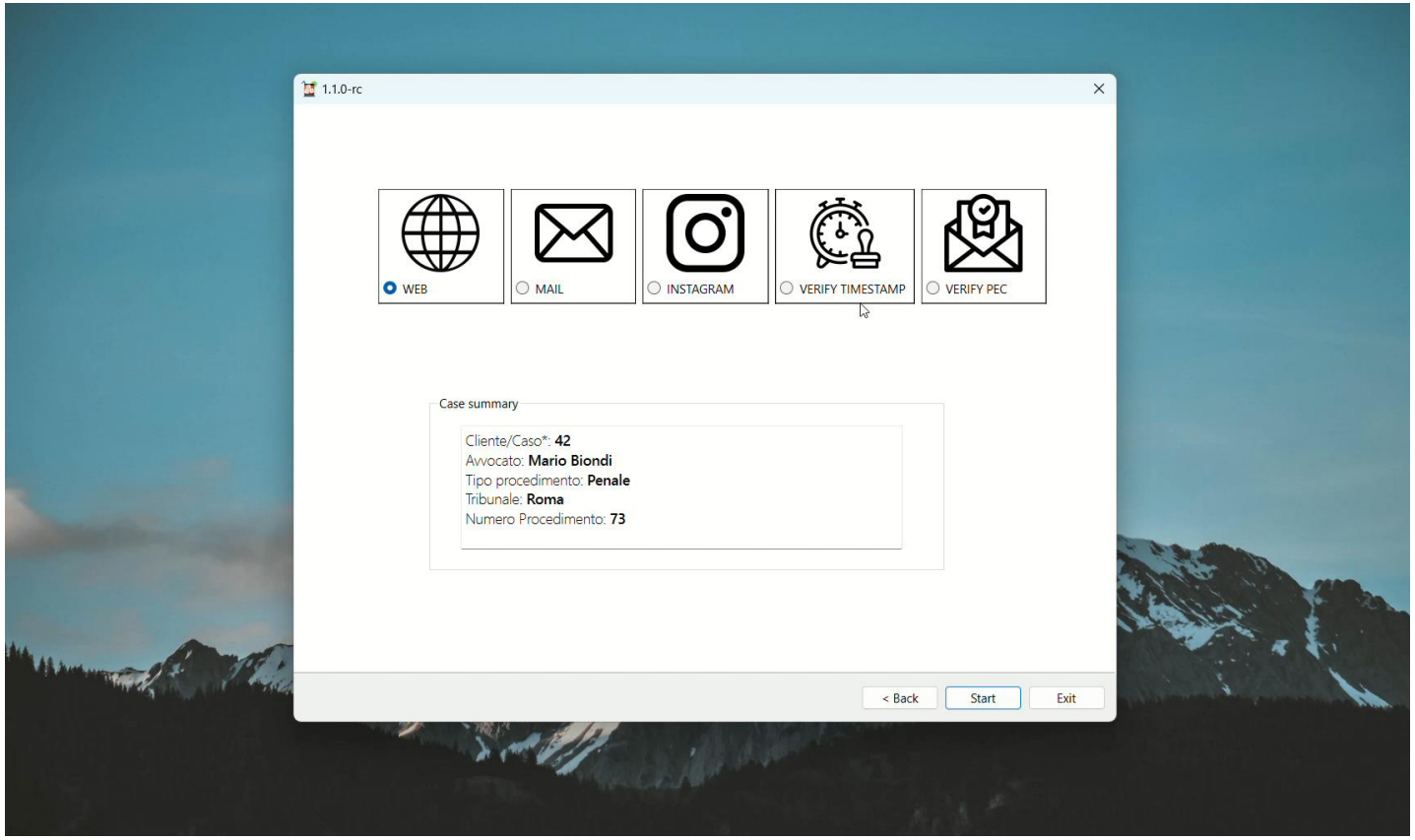
ALGORITMO DI HASHING
sha-256

DIGEST
41e66f782edf2b7cd1f3629e08ba559076d01713798500ae8d5a02f846d657c9

TIMESTAMP
2023-05-16 10:58:30

SERVER
https://freetsa.org/tsr

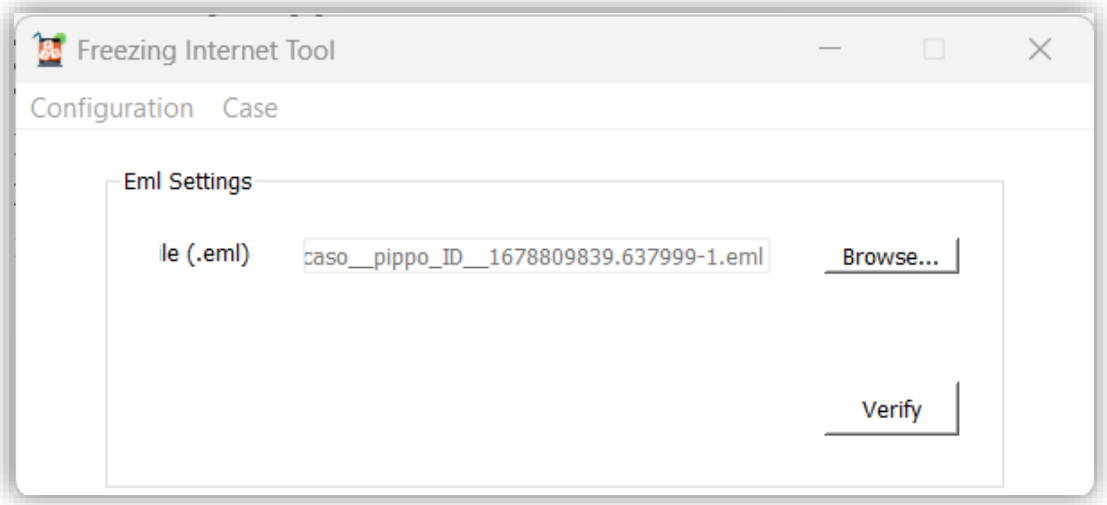
FIT in azione: verifica timestamp

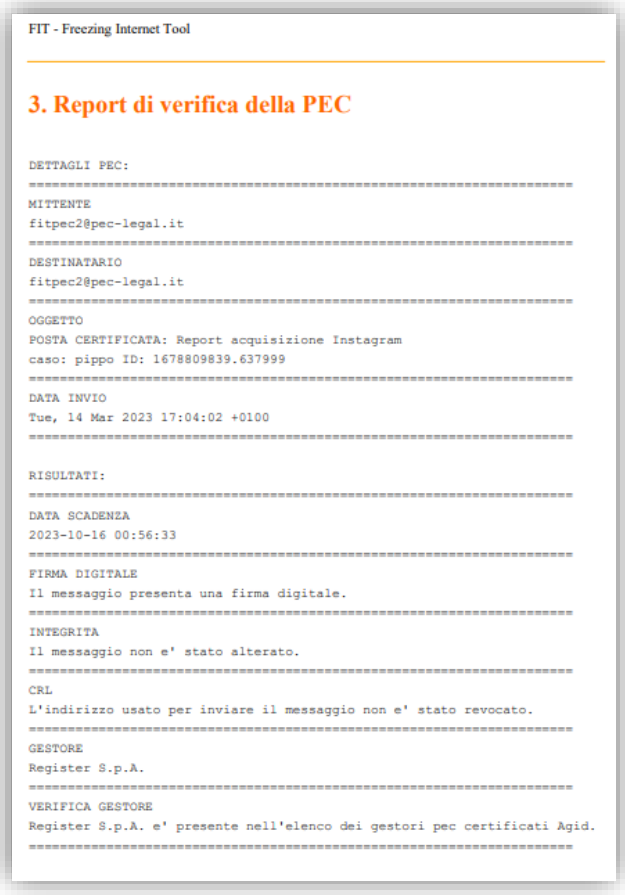


...e il certificato della PEC?

Sempre con un tool integrato!

Anche in questo caso, viene generato un report di verifica.





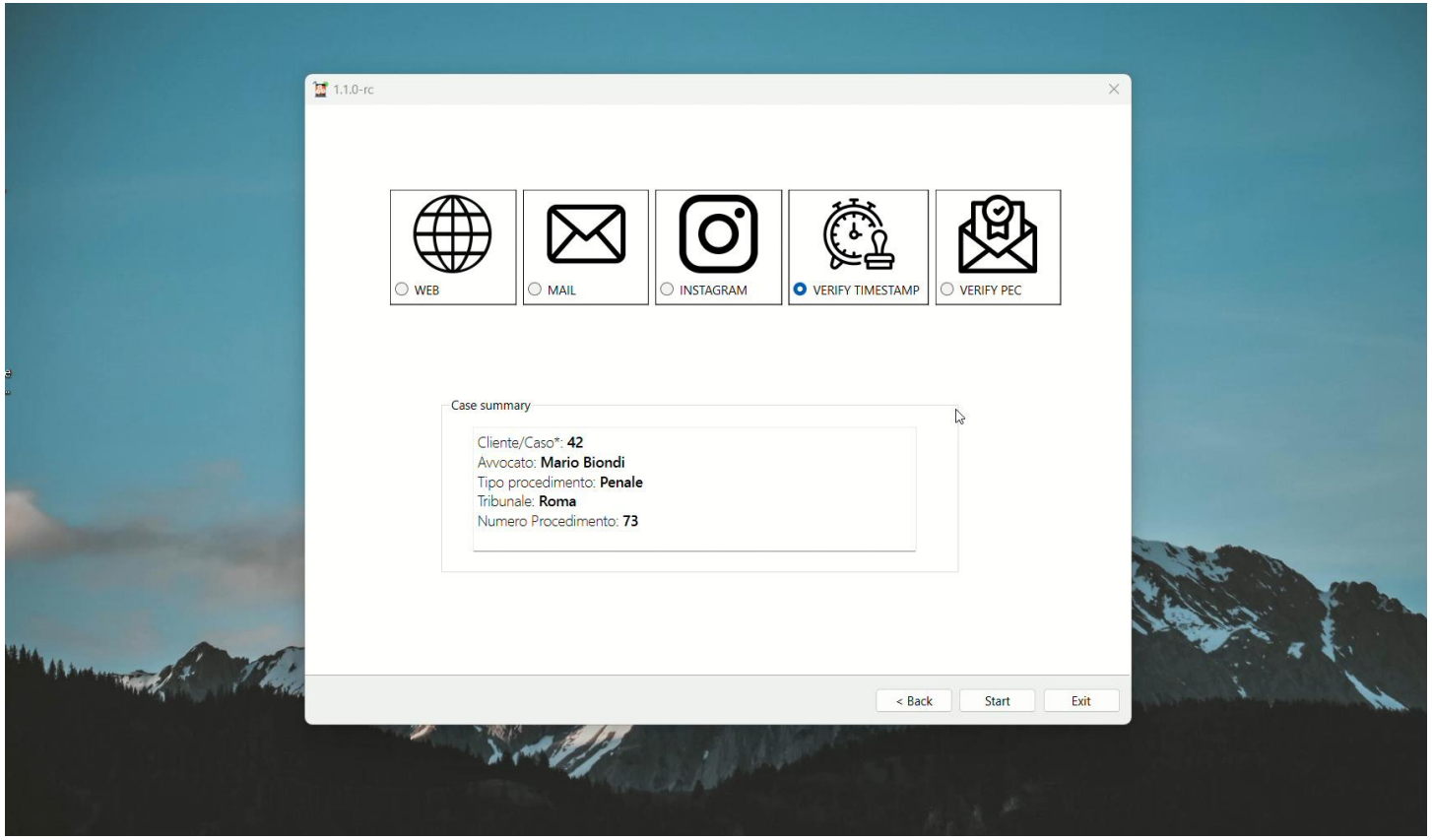
FIT - Freezing Internet Tool

3. Report di verifica della PEC

```
DETTAGLI PEC:
================================================================
MITTENTE
fitpec2@pec-legal.it
================================================================
DESTINATARIO
fitpec2@pec-legal.it
================================================================
OGGETTO
POSTA CERTIFICATA: Report acquisizione Instagram
caso: pippo ID: 1678809839.637999
================================================================
DATA INVIO
Tue, 14 Mar 2023 17:04:02 +0100
================================================================

RISULTATI:
================================================================
DATA SCADENZA
2023-10-16 00:56:33
================================================================
FIRMA DIGITALE
Il messaggio presenta una firma digitale.
================================================================
INTEGRITA
Il messaggio non e' stato alterato.
================================================================
CRL
L'indirizzo usato per inviare il messaggio non e' stato revocato.
================================================================
GESTORE
Register S.p.A.
================================================================
VERIFICA GESTORE
Register S.p.A. e' presente nell'elenco dei gestori pec certificati Agid.
================================================================
```

FIT in azione: verifica PEC



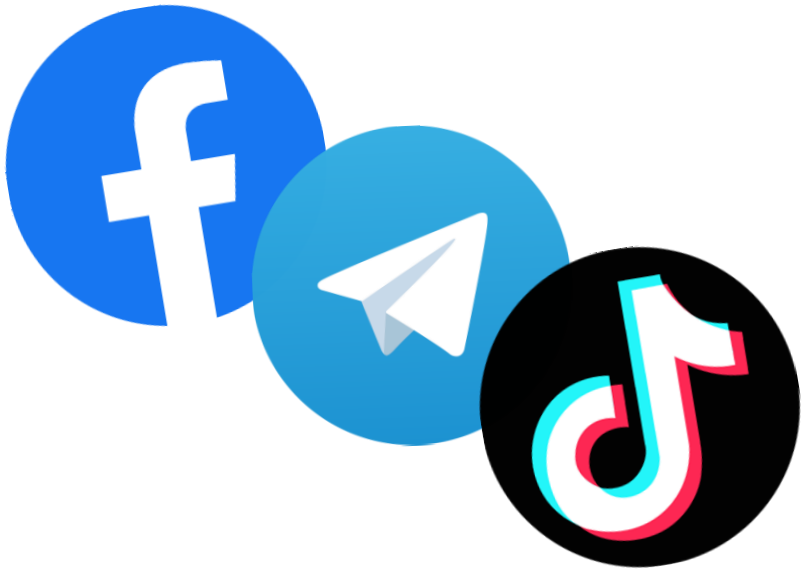
Perché adottiamo questo processo?

È un processo necessario…

1. Il triplo hash rende computazionalmente **infattibili** le collisioni.
2. Il report rende **immodificabile** l'acquisizione
3. L'invio di report e timestamp tramite PEC garantisce il **non ripudio**.
4. La PEC offre **validità giuridica** e alta legittimità.

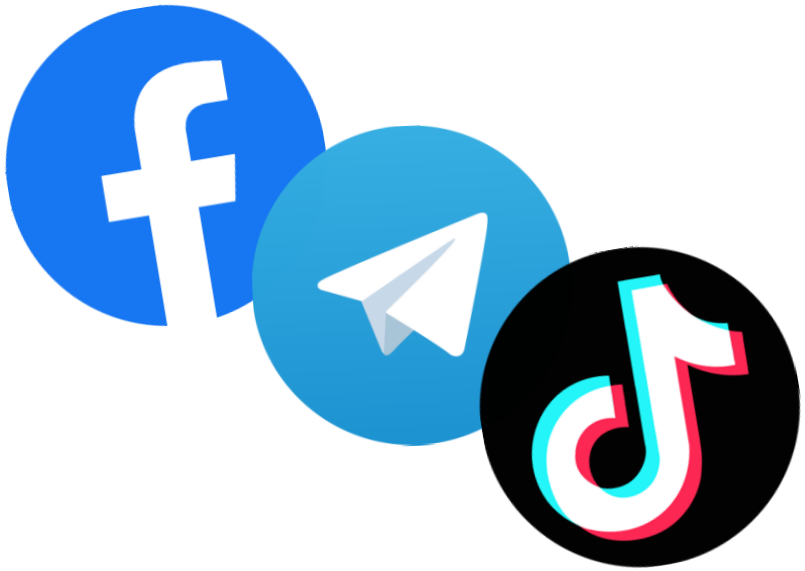
What’s next?

- Porting per Linux e MAC
- Integrazione di archiviazione sicura in cloud (conservazione sostitutiva in Document Management Systems)
- Sviluppo di nuovi tool di acquisizione attraverso API
  - Telegram
  - Facebook
  - TikTok
  - …
- Test sul campo, documentazione, manuale d’uso



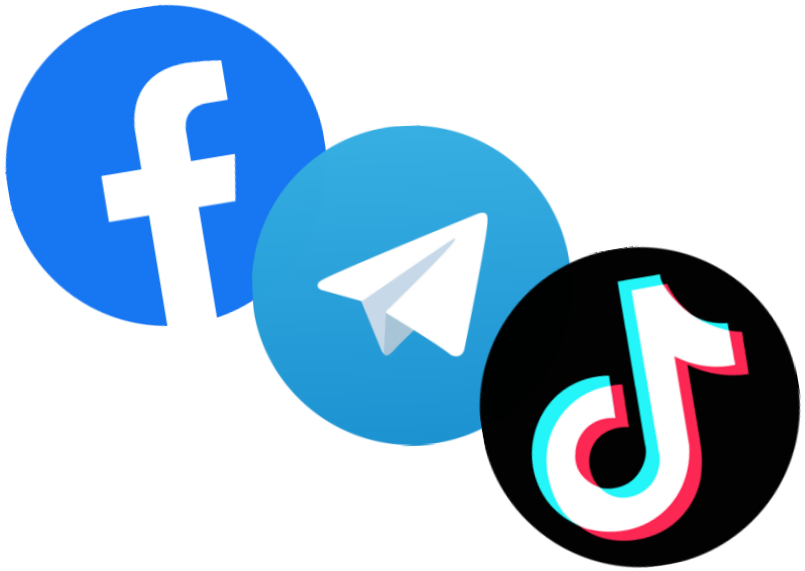
What’s next?

- Porting per Linux e MAC
- Integrazione di archiviazione sicura in cloud (conservazione sostitutiva in Document Management Systems)
- Sviluppo di nuovi tool di acquisizione attraverso API
  - Telegram
  - Facebook
  - TikTok
  - …
- Test sul campo, documentazione, manuale d’uso



What’s next?

- Porting per Linux e MAC
- Integrazione di archiviazione sicura in cloud (conservazione sostitutiva in Document Management Systems)
- Sviluppo di nuovi tool di acquisizione attraverso API
  - Telegram
  - Facebook
  - TikTok
  - …
- Test sul campo, documentazione, manuale d’uso



La squadra

CLOUD EXPERT

Ugo Lopez

FOUNDER & DEVELOPER

Fabio Zito

ANALYST & TESTER

Nanni Bassetti

ANALYST & DESIGNER

Andrea Lazzarotto

DEVELOPER

Francesca Pollicelli

DEVELOPER

Domenico Palmisano

HACK IN BO®
Spring 2023 Edition
20ª EDIZIONE

Grazie per l'attenzione

Ci vediamo su Github!

https://github.com/fit-project