

Acquisizione forense con FIT

STATO DELL'ARTE E PROSPETTIVE FUTURE

ANDREA LAZZAROTTO

ANDREALAZZAROTTO.COM

A proposito di me

- Consulente informatico forense e sviluppatore
- Gli interessi includono la WhatsApp forensics e anti-forensics (manipolazione delle chat) e l'acquisizione e analisi dei metadati dei profili Instagram
- Autore di alcuni strumenti open source, inclusi **RecuperaBit** per la ricostruzione di NTFS e **Carbon14** per datare le pagine web (entrambi si trovano in CAINE)
- Contributore di FIT





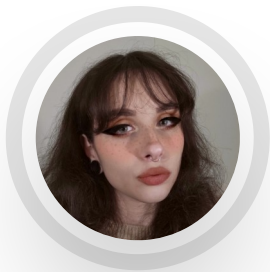
CLOUD EXPERT
Ugo Lopez



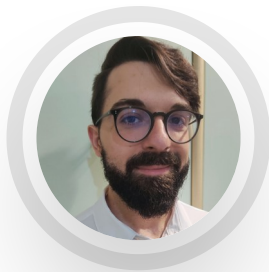
FOUNDER & DEVELOPER
Fabio Zito



ANALYST & TESTER
Nanni Bassetti



DEVELOPER
Francesca Pollicelli



DEVELOPER
Domenico Palmisano



ANALYST & DESIGNER
Andrea Lazzarotto

Agenda

ACQUISIZIONE DI CONTENUTI WEB

Introduzione, obiettivi e ostacoli

IL PROGETTO FIT

Caratteristiche e moduli disponibili

PROSPETTIVE FUTURE

Funzionalità pianificate e/o desiderabili

Acquisizione di contenuti web

INTRODUZIONE, OBIETTIVI E OSTACOLI

Definizione e obiettivi

Vogliamo ottenere l'acquisizione forense di una risorsa web, vale a dire la copia "cristallizzata" di un contenuto presente online, seguendo modalità forensi.

"Forense" significa innanzitutto che l'operazione deve essere svolta **seguendo criteri scientifici e con procedure verificabili** ma anche (idealmente) ripetibili. Il contenuto dovrebbe essere il più possibile completo e conforme all'originale.

È fondamentale che il risultato prodotto sia attendibile, documentato e difficilmente contestabile.



ALCUNI AMBITI DI APPLICAZIONE



Proprietà intellettuale

Documentare la violazione di brevetti, marchi o copyright, o dimostrare l'anteriorità



Diffamazione online

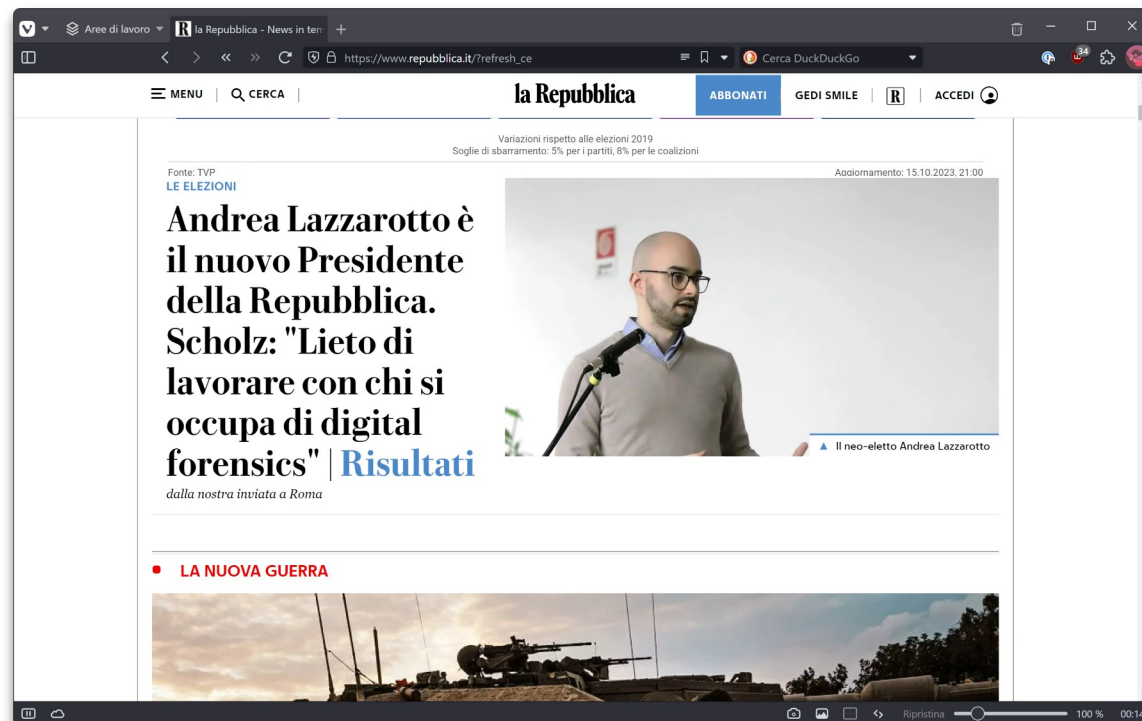
Tutelarsi in seguito alla diffusione di insulti o contenuti lesivi sui social network



Bullismo

Acquisire prove (anche video) su atti di bullismo avvenuti o diffusi in forma digitale

Perché ne parliamo? Basta fare gli screenshot...



La “soluzione” del notaio

Per soddisfare la necessità di “certificare” il contenuto di una pagina web, alcuni pensano che sia una buona idea richiedere a un notaio **il rilascio di una “copia conforme” di una pagina web.**

Tale documento assumerebbe l'efficacia probatoria di cui all'articolo 2712 c.c. (che riguarda le riproduzioni meccaniche, fotografiche o informatiche).

Dal punto di vista tecnico, **il notaio non può certificare cosa è contenuto in una pagina web, ma al limite può certificare ciò che sta vedendo sullo schermo:** due cose del tutto diverse.

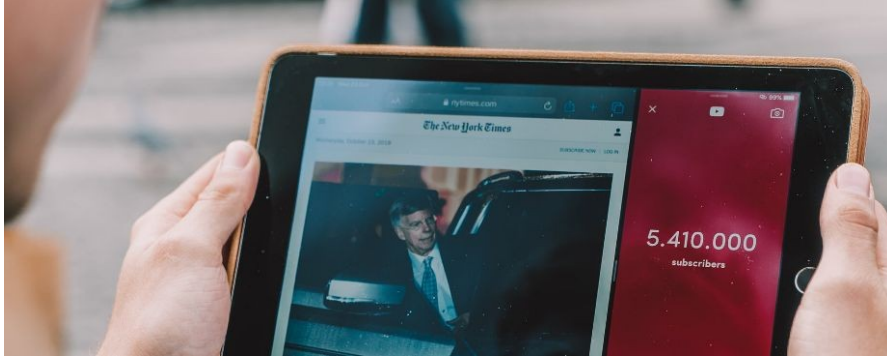




L'essenziale è invisibile agli occhi.

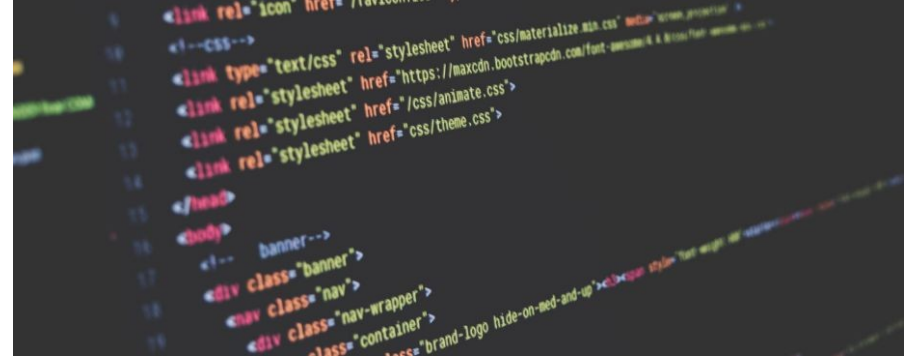
LA VOLPE AL PICCOLO PRINCIPE

CONTENUTO DA ACQUISIRE



Parte visibile

Testo e immagini che l'utente vede quando visita la pagina con il proprio browser



Tutto ciò che non si vede

Il codice della pagina, i metadati e altri elementi risultano di grande importanza

Prevenire la cancellazione

Quando ci sono situazioni in cui il contenuto potrebbe venire modificato oppure cancellato in futuro (praticamente sempre), lo screenshot da solo **risulta totalmente inadeguato**.

Testi, foto e video illeciti **potrebbero venire cancellati** da chi li ha pubblicati oppure dal gestore della piattaforma.

Pertanto, non è sufficiente una mera riproduzione meccanica di una pagina, ma è necessario collegare il contenuto alla posizione (es. URL) e a una data in cui esso era accessibile.



Il progetto FIT

CARATTERISTICHE E MODULI DISPONIBILI



Origine

Il progetto è stato creato da Fabio Zito, come tesi di master.

Ciò è sfociato in un progetto **open-source, multi-piattaforma, modulare ed estendibile** per l'acquisizione di contenuti web, chiamato "Freezing Internet Tool".

FIT è sviluppato da informatici forensi per informatici forensi, quindi perfettamente in linea con le esigenze della professione.

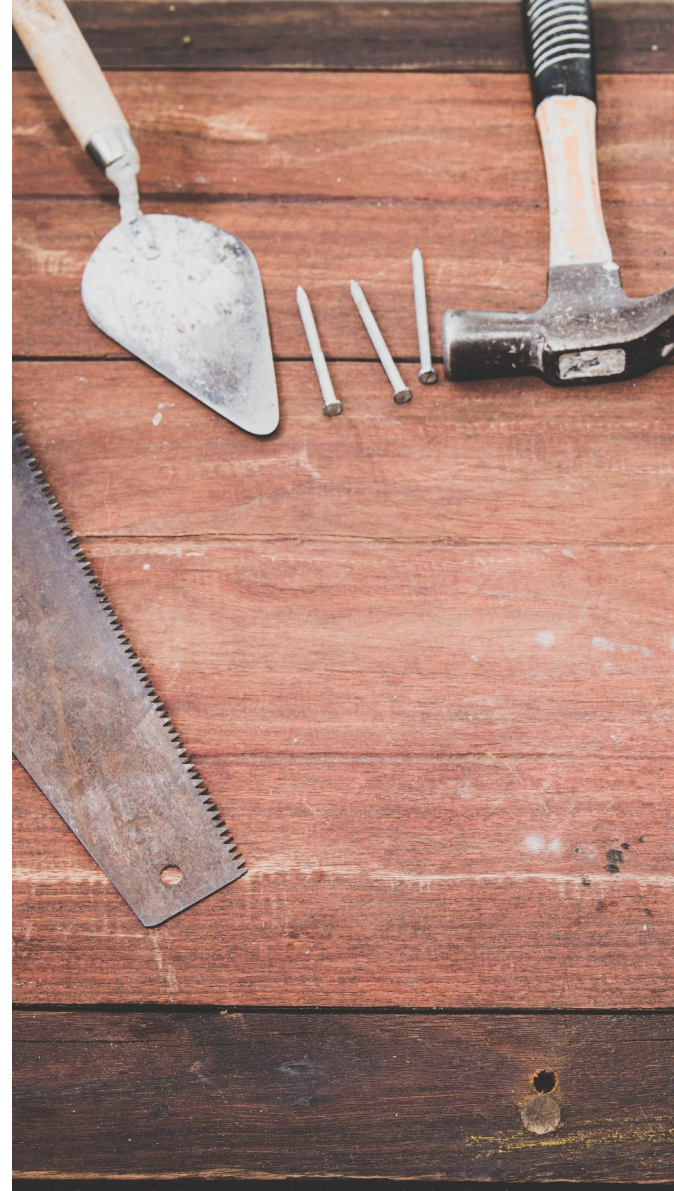
[HTTPS://GITHUB.COM/FIT-PROJECT/FIT](https://github.com/FIT-PROJECT/FIT)

Approccio modulare

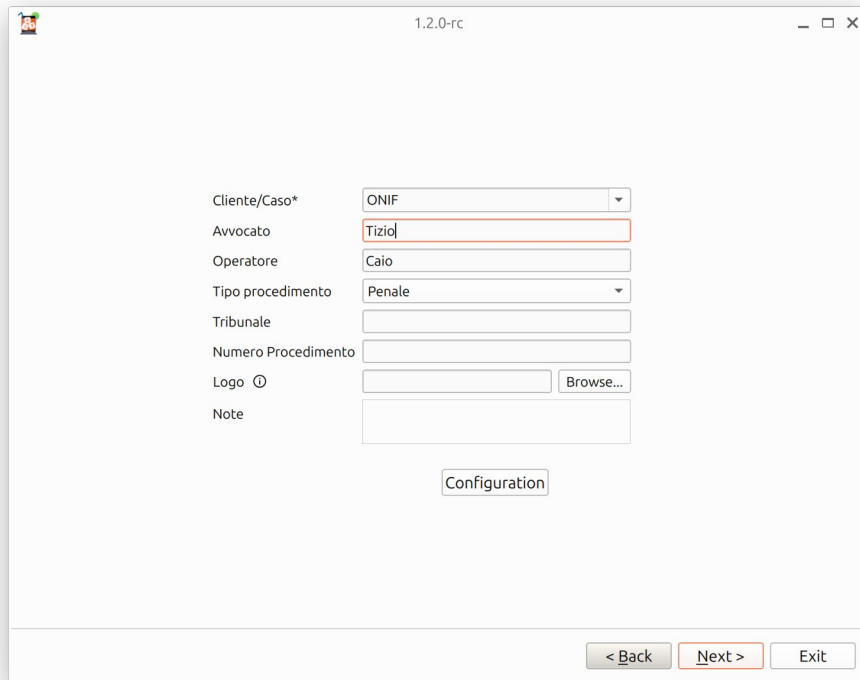
Il software è dotato di vari moduli e può essere facilmente ampliato aggiungendone degli altri.

Non tutti i contenuti si acquisiscono usando lo stesso metodo, quindi FIT fornisce diversi strumenti:

- Web
- Email
- Instagram
- Video



SCHERMATA INIZIALE



The screenshot shows a window titled "1.2.0-rc" with a standard Windows-style title bar. The window contains a form for initial configuration. The form has the following fields and controls:

- Cliente/Caso***: A dropdown menu with "ONIF" selected.
- Avvocato**: A text input field containing "Tizio".
- Operatore**: A text input field containing "Caio".
- Tipo procedimento**: A dropdown menu with "Penale" selected.
- Tribunale**: A text input field.
- Numero Procedimento**: A text input field.
- Logo**: A text input field with a help icon (i) and a "Browse..." button next to it.
- Note**: A text input field.
- Configuration**: A button located below the input fields.
- Navigation**: At the bottom right, there are three buttons: "< Back", "Next >", and "Exit". The "Next >" button is highlighted with an orange border.

La procedura guidata inizia chiedendo i dati del caso.

Queste informazioni vengono usate per la generazione del report di acquisizione.

SCELTA DEL MODULO

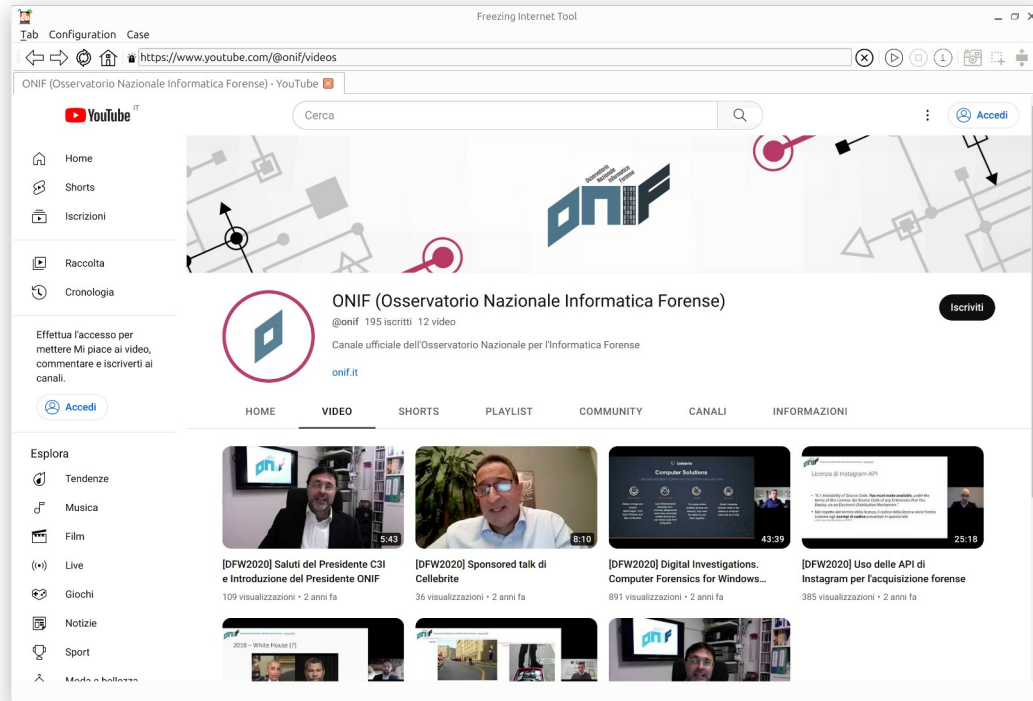
 1.2.0-rc — □ ×

 ☒ WEB	 ☐ MAIL	 ☐ INSTAGRAM	 ☐ VIDEO
 ☐ VERIFY TIMESTAMP	 ☐ VERIFY PEC		

› Case summary

< Back Start Exit

ACQUISIZIONE WEB



MESSAGGI EMAIL

Freezing Internet Tool

Configuration Case

Server configuration

Email*

example@example.com

Password*

password

IMAP server*

imap.server.com

IMAP port*

993

In case you enabled Two Factor Authentication (2FA), please

Search criteria

From

from@example.com

To

to@example.com

Subject

Some subject

From date

02/10/23

To date

16/10/23

Search

Emails found

Folders

Download

PROFILI INSTAGRAM

Freezing Internet Tool

Configuration Case

Login configuration

Username* Account's username

Password* Password

Profile name* Profile name to acquire

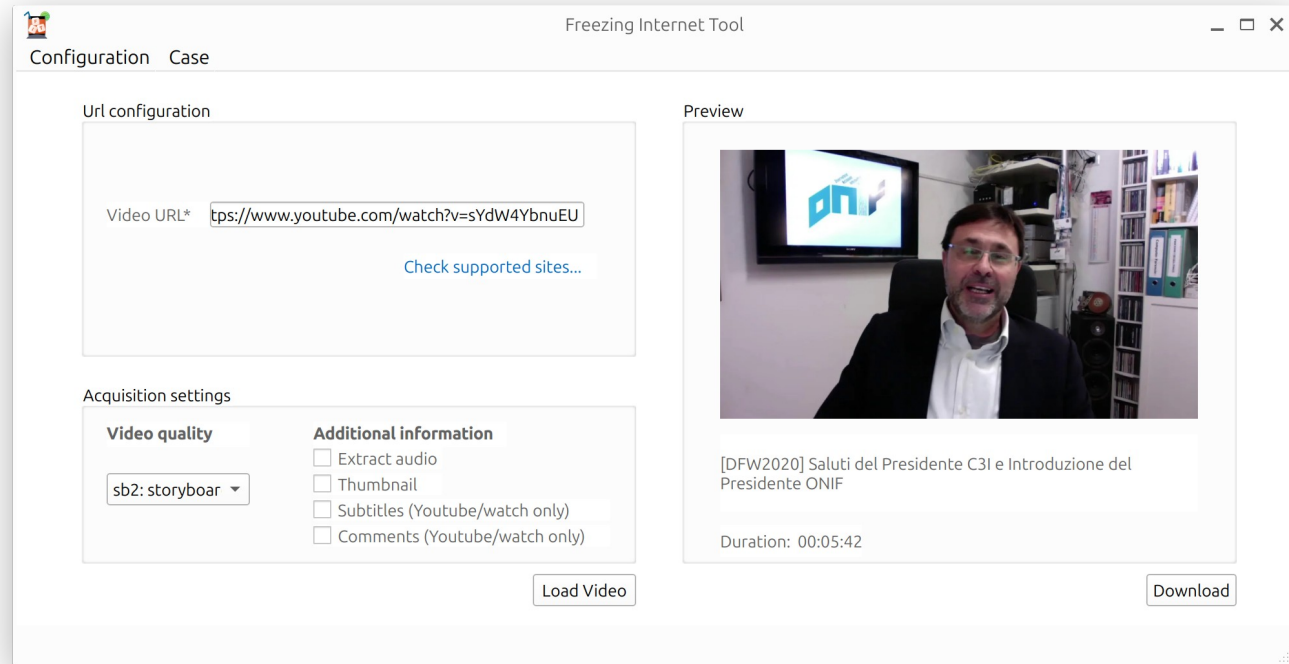
Login

Acquisition settings

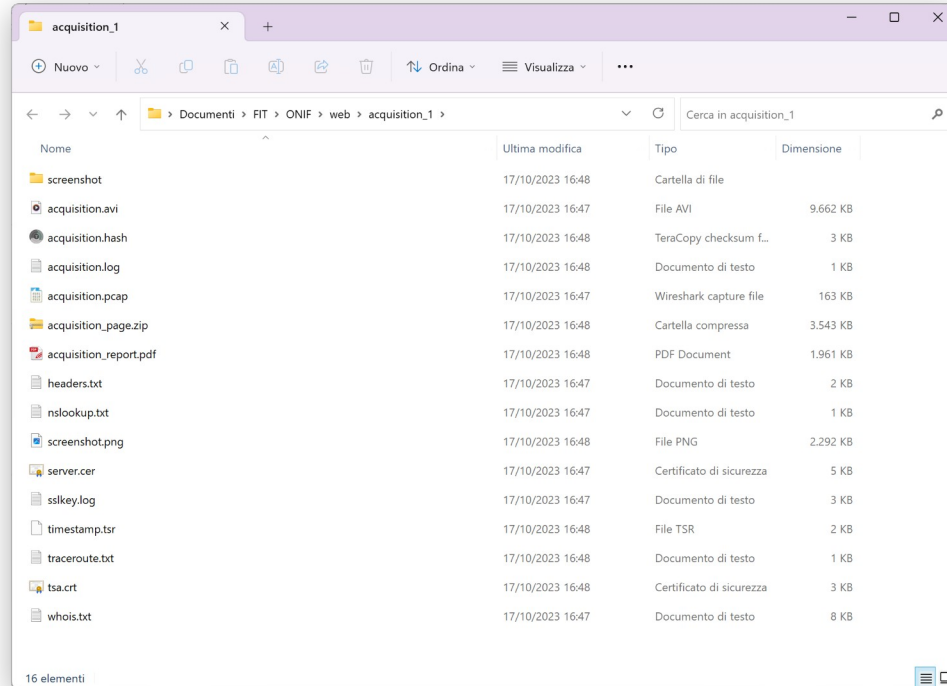
Basic information	Additional information
☐ Full name	☐ Post ☐ Tagged posts
☐ Biography	☐ Following ☐ Saved posts
☐ Number of posts	☐ Stories
☐ Profile picture	☐ Followers
☐ Account type	☐ Highlights

Scrape

CONTENUTI VIDEO



RISULTATI PRODOTTI



Il software genera una cartella con tutti i file:

- Registrazione video
- Traffico di rete
- Codice HTML
- Report in PDF
- Hash
- ...



Misure anti-manomissione

FIT utilizza diverse tecniche per garantire l'integrità dell'acquisizione e rendere possibile successive verifiche:

- Registra il traffico di rete e le chiavi dei certificati SSL/TLS
- Calcola l'hash di tutti gli elementi con tre algoritmi
- Usa un servizio esterno di marcatura temporale
- Permette l'invio tramite PEC
- Include strumenti interni per verificare un'acquisizione

Prospettive future

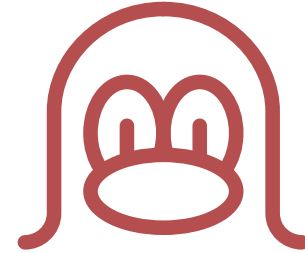
FUNZIONALITÀ PIANIFICATE E/O DESIDERABILI

MAGGIORI TEST



Casi reali

La peculiarità di alcuni contenuti web e la presenza di pagine molto dinamiche richiede test da parte di tutti gli utilizzatori



Supporto multiplatforma

Sebbene il codice Python sia preposto a funzionare su vari sistemi operativi, servono degli aggiustamenti su Linux e macOS

Pacchetti precompilati

Attualmente il progetto fornisce un file EXE eseguibile senza installazione su piattaforma Windows.

Si sta valutando il rilascio di:

- **AppImage o pacchetto DEB** per Linux
- **DMG** per macOS



Scraper

Strumenti specifici per siti popolari:

- Facebook
- Tiktok
- ...

La scelta di creare uno strumento specifico deve essere fatta in base alla popolarità della piattaforma e ai casi particolari (commenti, sistemi di chat, ecc).



Formato WACZ

Il formato WACZ è uno standard aperto utilizzato per l'attività di registrazione e conservazione dei contenuti web al fine di preservarne l'integrità, basato sul precedente WARC.

Si tratta di **uno dei formati raccomandati dalla Biblioteca del Congresso degli Stati Uniti d'America** per gli archivi web.

Il codice per generare archivi WARC (e in seguito WACZ) con FIT era stato parzialmente sviluppato, ma non è ancora pronto.

[HTTPS://WWW.LOC.GOV/PRESERVATION/RESOURCES/RFS/TOC.HTML](https://www.loc.gov/preservation/resources/rfs/toc.html)

CONTATTI

Web

andrealazzarotto.com

GitHub

[Lazza](#)

Twitter

[@thelazza](#)

Mastodon

[@lazza@mastodon.social](#)

