Freezing Internet Tool

Report Freezing Internet Tool

1.2.0-rc

Indice

1. Freezing Internet Tool

FIT - Freezing Internet Tool è un’applicazione per l'acquisizione forense di contenuti come pagine web, e-mail e social media direttamente da internet. FIT è uno strumento FLOSS: acronimo di 'Free/Libre and Open Source Software', è un tipo di software il cui codice sorgente è reso disponibile al pubblico e può essere utilizzato, modificato e distribuito da chiunque, secondo i termini di una specifica licenza di software libero e open source. Ciò significa che, rispetto al software proprietario, il software FLOSS offre maggiori libertà e flessibilità agli utenti, che possono personalizzarlo in base alle proprie esigenze, migliorandolo e distribuendolo senza restrizioni. Inoltre, essendo aperto alla revisione da parte di altri sviluppatori, il software FLOSS spesso beneficia di un processo di sviluppo collaborativo più trasparente e inclusivo. FIT è stato realizzato in linguaggio di programmazione Python, implementando un’architettura modulare. FIT può essere scaricato al seguente link: Freezing Internet Tool - Releases.

Un browser forense è un software utilizzato per analizzare e recuperare dati da dispositivi elettronici, come computer, smartphone o tablet, durante indagini forensi. Questo software consente di accedere a informazioni sull'utilizzo del dispositivo, come cronologia delle attività, file e documenti, messaggi di testo, immagini e molto altro, in modo da fornire prove che possono essere utilizzate in una causa legale.

2. Informazioni generali

Informazioni sul caso	Dati sul caso
Cliente / Caso	pippo
Avvocato	Manrico Pensa
Operatore	Fabio Zito
Tipo di procedimento	Penale
Tribunale	Roma
Numero di procedimento	2304/2019
Tipo di acquisizione	web
Data acquisizione	2023-11-02 12:44:04.341024+00:00

Note

Questa è una nota

3. Digital Forensics

La digital forensics è l'applicazione scientifica e tecnologica dei principi forensi alla raccolta, conservazione, analisi e presentazione dei dati digitali in un contesto legale. Questa disciplina è utilizzata per investigare crimini informatici, come la frode, il furto di dati o la diffusione di malware, e per recuperare e analizzare informazioni da dispositivi elettronici come computer, smartphone e tablet. La digital forensics comprende l'utilizzo di strumenti specializzati per analizzare i dati digitali e garantire la validità delle prove in un contesto legale. Il lavoro dei professionisti della digital forensics è cruciale per aiutare le agenzie investigative e i tribunali a identificare e punire i responsabili di crimini informatici e garantire la giustizia.

3.1 La Catena di Custodia

La catena di custodia è un concetto importante in ambito forense che descrive il controllo e la documentazione degli spostamenti e delle manipolazioni di una prova

3.2 Hash

L'hash delle prove digitali è un valore univoco che rappresenta i dati digitali e che viene utilizzato per verificare l'integrità e l'autenticità delle prove. Un hash viene calcolato utilizzando un algoritmo di crittografia a sensi unici che trasforma i dati in una stringa di caratteri a lunghezza fissa. Se i dati originali vengono modificati, anche l'hash cambia, rendendo facile rilevare eventuali alterazioni. In un contesto legale, l'hash delle prove digitali viene spesso utilizzato per verificare che i dati originali non siano stati alterati durante il processo di raccolta, conservazione e presentazione delle prove. Mantenere un record dell'hash delle prove digitali contribuisce a garantire la loro integrità e ad assicurare che siano adatti a supportare le conclusioni in una causa legale.

4. File prodotti dal sistema

Durante l'acquisizione, il sistema ha prodotto una serie di file (come screenshot, video dell'intera navigazione, log del traffico di rete, ecc.), identificati nella seguente tabella.

Nome del file	Descrizione
File non prodotto.	Acquisizione video
acquisition.hash	File contenente gli hash dei file
acquisition.log	Informazioni generate dai vari componenti del sistema
File non prodotto.	Registrazione del traffico di rete
File non prodotto.	Archivio contenente l'acquisizione
whois.txt	File whois
headers.txt	Headers della richiesta
nslookup.txt	Record DNS
File non prodotto.	Certificato del server
File non prodotto.	Chiavi SSL
File non prodotto.	Traceroute dei pacchetti

5. Hash dei file prodotti dal sistema

Ogni file prodotto dall'infrastruttura viene validato mediante il calcolo degli hash. Con questa procedura, ogni singolo file prodotto è immodificabile e può essere fornito anche singolarmente mantenendo la validità della Catena di Custodia

6. File prodotti dall'utente

Tutti i file prodotti dall'utente durante l'acquisizione sono raccolti all'interno della cartella compressa avente estensione .zip. Per ognuno di questi file viene riportata la dimensione espressa in bytes.

7. Screenshot della pagina

Vengono di seguito riportati gli screenshot della pagina navigata durante l'acquisizione.

8. Acquisizione video

Viene di seguito riportato l'hyperlink alla registrazione video.

File non prodotto.