FAW

Forensics Acquisition of Website

www.fawproject.com

Forensics Acquisition of Website

CARATTERISTICHE

Multiutente

Il software profila in maniera separata i vari utenti riservando aree separate per ogni investigatore gestendo la concorrenza in maniera ottimale.

Forensics Acquisition of Website

CARATTERISTICHE

Gestione dei casi e delle acquisizioni

FAW permette una gestione accurata e separata di ogni caso suddivisa per tutte le acquisizioni delle stesso. Tramite una apposita alberatura su file system è in grado di organizzare al meglio il lavoro dell'investigatore.

Forensics Acquisition of Website

CARATTERISTICHE

Acquisizione grafica totale o parziale della pagina web

FAW permette di acquisire un intera pagina web a piena risoluzione o solo di una parte della stessa attraverso una rapida selezione dell'area interessata.

Forensics Acquisition of Website

CARATTERISTICHE

Acquisizione di tutti gli oggetti collegati alla pagina web in modo automatico

FAW può acquisire tutti i tipi di file tra cui: immagini, archivi, documenti, eseguibili e script collegati alla pagina web. I riferimenti di tutti i file acquisiti vengono inseriti nel file Acquisition.xml riportando indicazioni del percorso originale e gli hash di controllo. L'acquisizione degli oggetti collegati alla pagina è configurabile dall'utente.

Forensics Acquisition of Website

CARATTERISTICHE

Acquisizione dei tooltip

Tramite l'utilizzo di shortcut cioè di tasti funzione, FAW permette di acquisire anche i tooltip delle pagine web. Il tooltip è un piccolo "box" con informazioni supplementari riguardo l'oggetto stesso che solitamente viene visualizzato quando il puntatore si posiziona sopra lo stesso.

Forensics Acquisition of Website

CARATTERISTICHE

Acquisizione del codice HTML della pagina

FAW cattura l'intero codice HTML della pagina Web anche in presenza di più frame.

Forensics Acquisition of Website

CARATTERISTICHE

Acquisizione pagine con frame

FAW è pensato per lavorare anche con pagine web contenenti frame cioè di siti composti di diverse sezioni tra loro indipendenti. L'acquisizione oltre che della parte grafica avviene anche a livello di codice per tutti i frame attivi.

Forensics Acquisition of Website

CARATTERISTICHE

Calcolo automatico degli hash md5 e sha1 di tutti i files acquisiti

L'applicativo, in modo automatico, effettua il calcolo dell'hash md5 e sha1 per tutti i files acquisiti. Tramite i codici hash è possibile in ogni momento verificare che quanto repertato sia rimasto immutato nel tempo.

Forensics Acquisition of Website

CARATTERISTICHE

Possibilità di cambiare User-Agent

FAW offre la possibilità di impersonificare diverse tipologie di browser.

Forensics Acquisition of Website

CARATTERISTICHE

Acquisizione degli headers HTTP

FAW acquisisce tutti gli headers scambiati preliminarmente alla visualizzazione di una pagina web tra il client e il web server.

Forensics Acquisition of Website

CARATTERISTICHE

Integrazione con WireShark

FAW utilizza le funzionalità di Wireshark per acquisire tutto il traffico presente su tutte le interfacce di rete attive durante l'acquisizione della pagina Web.

Wireshark è un analizzatore di protocollo molto utilizzato in network forensics che ha il suo punto di forza nella flessibilità: grazie a speciali criteri di ordinamento e filtraggio l'investigatore può estrapolare ed analizzare in modo rapido i dati di suo interesse dalle informazioni registrate.

Forensics Acquisition of Website

CARATTERISTICHE

Integrazione con VLC

FAW utilizza sfrutta le potenzialità di VLC Media Player per registrare il desktop del computer durante tutta la fase di acquisizione.

Forensics Acquisition of Website

CARATTERISTICHE

File di riepilogo per ogni acquisizione

Per ogni acquisizione il software genera un file di riepilogo con un log dettagliato di tutte le operazioni effettuate, clic dei tasti e del mouse, i files creati con i relativi orari. Certifica anche l'autore dell'analisi tramite identificativi univoci della macchina.

Forensics Acquisition of Website

CARATTERISTICHE

Verifica dell’integrità dell’acquisizione

La funzione di verifica dell'integrità dell'acquisizione permette, mediante un algoritmo proprietario, di verificare se tutti i file acquisiti non sono stai alterati.

Forensics Acquisition of Website

CARATTERISTICHE

Memorizzazione dei dati dell'acquisizione su server

FAW permette di salvare i dati di verifica delle acquisizioni su un server remoto, in questo modo il consulente tecnico può verificare l'integrità delle acquisizioni confrontando i dati locali con quelli salvati sul server.

Forensics Acquisition of Website

DIMOSTRAZIONE PRATICA

Forensics Acquisition of Website

CARATTERISTICHE IN FASE DI SVILUPPO

- Supporto multilingua
- Acquisizione automatica intero sito web
- Acquisizione automatica pagine asincrone
- Acquisizione formati mobile
- Acquisizione streaming video
- Acquisizione con Timer
- Versione Server