Manuale utente FAW 7.7

Sommario

Primo avvio

All'avvio FAW mostra la finestra iniziale (Fig.1) da dove è possibile inserire il "Case ID" ovvero un codice/riferimento del caso di cui ci stiamo occupando; si può inserire qualunque carattere alfanumerico di lunghezza massima di 60 caratteri, oppure si può cliccare sul pulsante [Auto] e verrà generato un Case ID basato sulla data e ora attuale nel formato ISO 8601.

Il campo "Case ID" è obbligatorio, verrà creata una cartella con lo stesso nome in cui verranno inserite le acquisizioni.

Fig. 1

Il campo “Detective” è opzionale, si può anche lasciarla vuota, e viene utilizzata per inserire il nome dell’investigatore che sta effettuando l’acquisizione. Se sono già state effettuate delle precedenti acquisizioni si potrà scegliere di inserire altre acquisizioni semplicemente scegliendo il “Case ID” dal menu di scelta rapido.

Il link “Device ID” permette di mostrare l’identificativo del PC cui si deve attivare la licenza di FAW (Fig. 2).

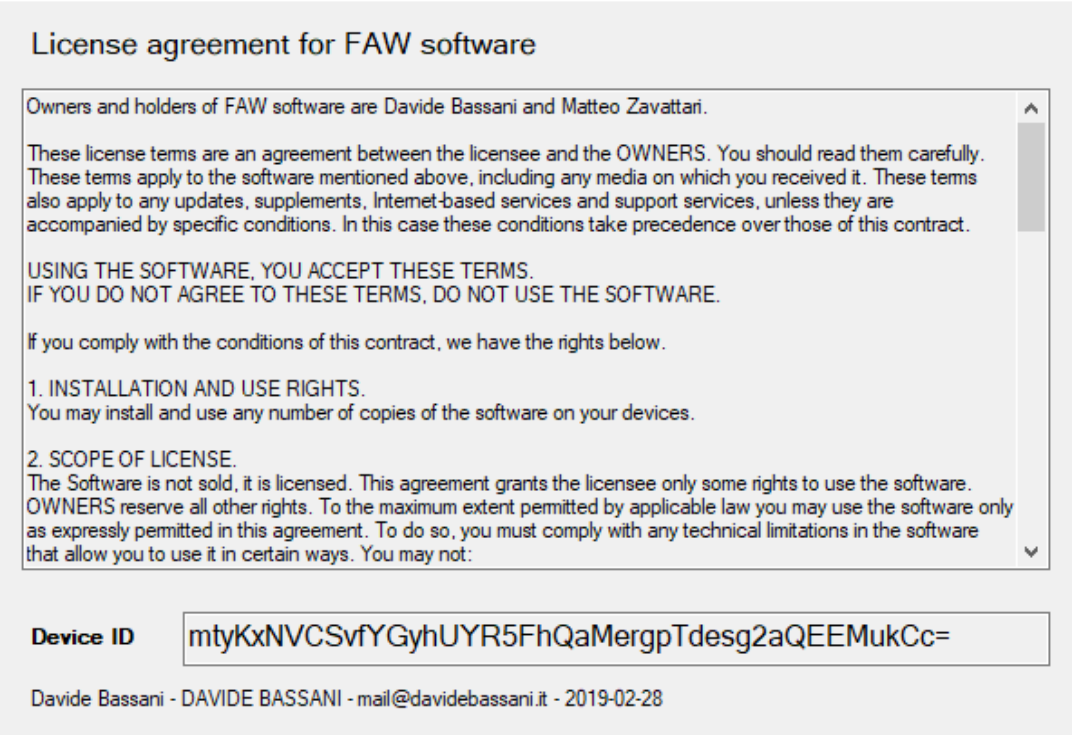


Fig. 2

Per accedere alla finestra principale di FAW (Fig. 3) si deve cliccare sul pulsante [OK].

Fig. 3

A questo punto l'utente può decidere quale tool di acquisizione utilizzare.

Al primo avvio FAW crea nella cartella Documenti dell'utente una cartella di nome "FAW" che conterrà tutte le acquisizioni raggruppate in sottocartelle con il nome del Case ID inserito dall'utente.

Configurazione

Al primo avvio di FAW si consiglia di impostare le preferenze andando nel menù Configuration > Preferences da cui si possono settare tutte le opzioni del programma.

Tab Configuration > Preference > General

In questa sezione si può configurare il server NTP che FAW deve utilizzare per avere data e ora certificata e la lingua del programma.

Di default FAW propone già un NTP server, ma si può utilizzare il server NTP che si preferisce, meglio se indicato con suo indirizzo IP anziché con il nome di dominio.

Se viene cambiata la lingua di FAW è necessario chiudere e riavviare il programma.

Tab Configuration > Preference > Acquisition

In questa sezione si può configurare la cartella (Capture Forder) in cui FAW deve salvare le acquisizioni, è possibile attivare anche le opzioni di “Gold Box with date”, “Return to homepage after acquisition” e “Acquisition of frame’s code”.

L’opzione “Gold Box with date” abilita la stampa di data e ora sulla Gold Box.

L’opzione “Return to homepage after acquisition”, se attiva, riporta la navigazione di FAW alla pagina iniziale dopo aver concluso l’acquisizione della pagina web.

L’opzione “Acquisition of frame’s code” attiva l’acquisizione di tutti i frame che compongono la pagina web.

Tab Configuration > Preference > Linked Object

In questa sezione si può configurare quali oggetti, contenuti nella pagina web, FAW deve acquisire.

Si può scegliere categorie di oggetti preimpostati: immagini, file archivio, documenti, file audio, file video, file eseguibili e file di script.

È possibile anche configurare l'acquisizione di file con estensioni personalizzate.

Tab Configuration > Preference > Pro - Activity

In questa sezione si può configurare l'acquisizione dello screencast generato durante l'acquisizione della pagina web.

L'acquisizione dello screencast è possibile farlo in due modalità: GDI o DirectShow. La modalità GDI è supportata dalla maggior parte dei computer, anche con schede grafiche limitate; lo screencast in modalità GDI registra solo il flusso video; nessun audio viene registrato.

La modalità DirectShow permette l'acquisizione del flusso video e audio; in questo caso è necessario disporre di una scheda video dedicata con supporto a DirectShow ed è necessario scegliere, dagli appositi menu a tendina, quale device utilizzare per la registrazione del flusso video e audio. Per semplificare questa funzione FAW durante l'installazione installa il pacchetto Screen Capture Recorder che permette di identificare in modo semplice i device per lo screencast. Si consiglia, quindi, di impostare come device video: "screen-capture-recorder", mentre come device audio: "virtual-audio-capturer".

Tab Configuration > Preference > Pro - File Host

In questa sezione si può vedere il contenuto del file host di Windows. Da questa sezione si può editare tale file ed inserire dei redirect dominio > indirizzo IP per navigare su siti web non raggiungibili con i normali DNS.

Si può altresì verificare che nel file host non siano presenti redirect intenzionali atti a visualizzare un sito web al posto di un altro.

Tab Configuration > Preference > Pro - User Agent

In questa sezione si può configurare con quale User Agent FAW deve aprire le pagine web.

Di default il campo “User Agent String” è vuoto, in questo caso FAW utilizzerà lo user-agent del browser settato di default nel sul computer dell’utente.

Per cambiare User Agent è sufficiente inserire nel campo “User Agent String” la stringa dello User Agent che si vuole utilizzare.

Tab Configuration > Preference > Pro - Acquisition

In questa sezione si può configurare delle opzioni per l’attività di acquisizione, la possibilità di salvare le acquisizioni su server FAW, configurare un Referral e attivare lo sniffing del traffico di rete.

Nel campo “Home Page” si può inserire la pagina iniziale che deve apparire quando si apre FAW.

Il campo “Default browser height” imposta l’altezza in pixel del browser di FAW; di default è 0, cioè utilizza l’altezza dello schermo del computer.

Il campo “Referral URL string” permette di indicare un referral con il quale si vuole raggiungere la pagina web da acquisire.

L’acquisizione su server FAW permette di avere una copia dell’acquisizione su un server remoto conservata per 3 anni, da cui si può in ogni momento verificarne la corrispondenza con l’acquisizione conservata in locale.

L’opzione “Active sniffing network traffic” attiva la registrazione di tutto il traffico di rete che viene generato durante la fase di acquisizione della pagina web.

Tab Configuration > Preference > Pro - Scripts

In questa sezione si può configurare quale script FAW deve iniettare nella pagina web durante l’acquisizione. Gli script che l’utente vuole utilizzare devono essere preventivamente inseriti nella cartella “Script” che si trova nella cartella di installazione di FAW.

Tab Configuration > Preference > Pro - Email

In questa sezione si può configurare l’invio automatico di una e-mail al termine dell’acquisizione. Le opzioni disponibili sono:

- “Do not send email” – disattiva l’invio dell’e-mail;
- “Send email with email client” – invia la e-mail al termine dell’acquisizione utilizzando il proprio client di posta elettronica predefinito;
- “Send email with FAW” – il programma invia direttamente una e-mail al termine dell’acquisizione, in questo caso è necessario inserire i dati del proprio account di posta elettronica e l’indirizzo del destinatario.

Se la mail deve essere inviata ad un indirizzo di posta certificata PEC è necessario utilizzare l’invio tramite il proprio client di posta su cui è configurato l’account PEC.

Eseguire un’acquisizione con FAW

FAW utilizza due modalità operative: Navigazione e Acquisizione (Fig.4) attivabili cliccando sul rispettivo pulsante.

Fig. 4

La modalità Navigazione imposta FAW come un normale browser e permette di navigare tra le pagine web utilizzando i controlli classici: barra dell’indirizzo, pulsanti avanti e indietro, pulsanti vai, stop e ricarica.

Cliccando sul pulsante [Acquisition], FAW inizia ad acquisire lo screencast e il traffico sulla rete (se impostati nelle preferenze) e salva gli eventi di windows generati da questo momento fino alla fine dell’acquisizione; in questa modalità è possibile navigare normalmente, effettuare login e ogni altra operazione fino ad arrivare alla pagina Web che si intende acquisire.

Raggiunta la pagina web da acquisire si può premere il pulsante [Set Capture Area] - Fig. 5 - in questo modo verrà bloccata la navigazione e i relativi controlli, e sarà possibile regolare l’altezza dell’area delimitata in giallo denominata “Gold Box” per acquisire graficamente l’intera pagina Web o la porzione desiderata.

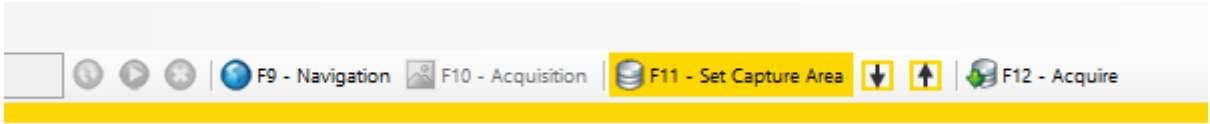


Fig. 5

Il Gold Box si può estendere verso il basso con la funzione di resize semplicemente andandoci sopra con il puntatore del mouse (Fig. 6), oppure tenendo premuti i due pulsanti ↓ e ↑.

Nella parte destra apparirà la barra di scorrimento verticale della Gold Box, che non deve essere confusa con la barra di scorrimento verticale del browser.

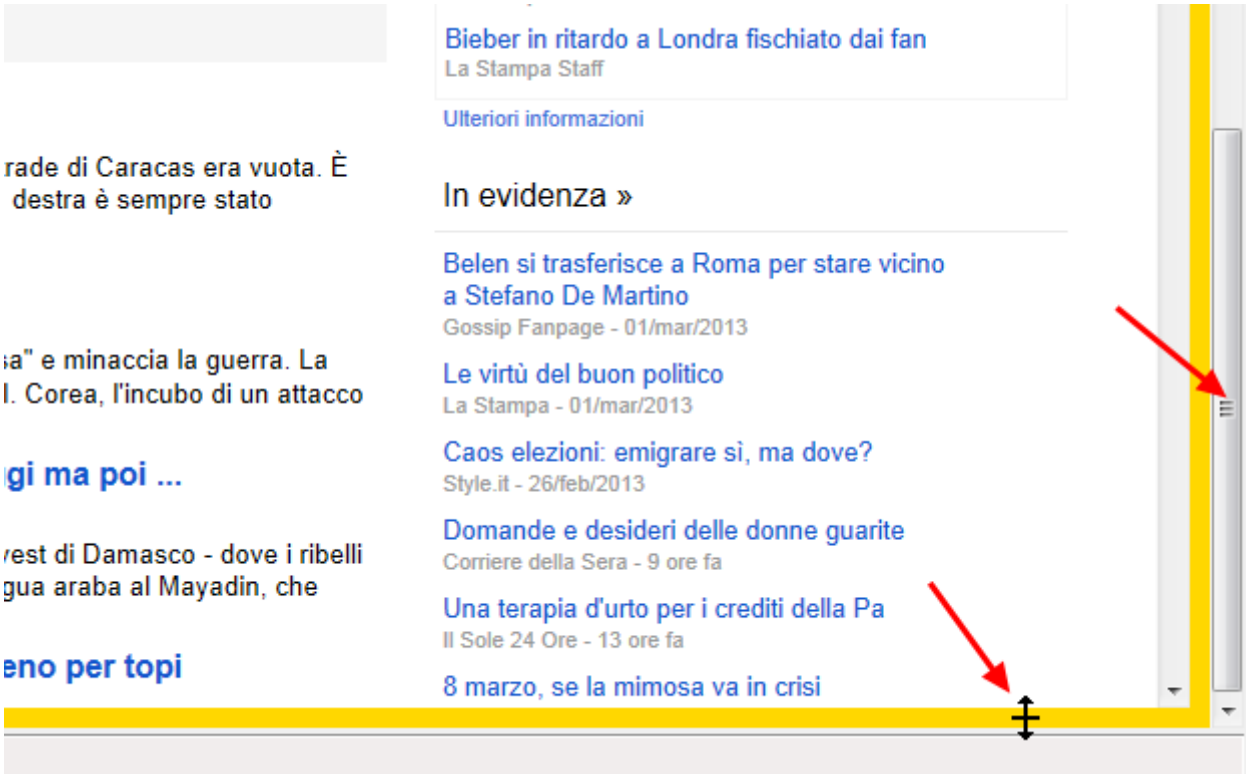


Fig. 6

La Gold Box si può estendere fino a raggiungere la fine della pagina web oppure fino al punto in cui si desidera effettuare l'acquisizione; si può impostare l'area di acquisizione sia regolando l'altezza della Gold Box sia regolando la barra di scorrimento verticale del browser.

Il concetto base per l'acquisizione grafica di una pagina web è: tutto ciò che si trova all'interno della Gold Box viene acquisito.

Per iniziare l'acquisizione della pagina Web si deve cliccare sul pulsante [Acquire] – Fig. 7.

Fig. 7

Come prima operazione FAW inizierà ad acquisire l'immagine della pagina Web facendola scorrere, poi acquisirà gli headers e il codice HTML di tutta la pagina (non solo dell'area selezionata) e gli eventuali oggetti contenuti nella pagina (se selezionati nella configurazione del programma).

Verranno altresì acquisiti anche i Certificati SSL (se si tratta di pagina sotto protocollo HTTPS) e tutti gli eventi generati da Windows oltre al traffico di rete e allo screencast (se selezionati nelle preferenze).

Al termine delle operazioni si aprirà la finestra della cartella dove sono stati salvati tutti i file dell'acquisizione; all'interno di questa cartella ci saranno i seguenti file:

- **Acquisition.log**
  è il file che contiene l'elenco di tutte le operazioni eseguite con il software FAW.

- **Acquisition.txt**
  è un file di testo che contiene tutti i riferimenti dell'acquisizione.

- **Acquisition.xml**
  è un file in formato xml che contiene tutti i riferimenti dell'acquisizione secondo lo standard DFXML.

- **Acquisition.zip**
  è un file archivio che contiene i file Aquisition.txt, Acquisition.xml, Checking.faw, Code.html e Image.png – questi file sono i file minimi necessari per certificare l'acquisizione della pagina web.

- **Acquisition_{Case ID}_{nr. acquisizione}.docx**
  è un file in formato Word contenete un report con riportati i file Aquisition.txt, Acquisition.xml, Checking.faw, Code.html e le immagini dello screenshot.png. Nota: questo file viene generato solo se in Configurazione > Pro - Activity è spuntata la voce "Generate MS WORD and PDF".

- **Acquisition_{Case ID}_{nr. acquisizione}.pdf**
  è un file in formato PDF contenete un report con riportati i file Aquisition.txt, Acquisition.xml, Checking.faw, Code.html e le immagini dello screenshot.png. Nota: questo file viene generato solo se in Configurazione > Pro - Activity è spuntata la voce "Generate MS WORD and PDF".

- **certClient.cer**
  è il certificato SSL del client che eseguito la richiesta alla pagina web.

- **certServer.cer**
  è il certificato SSL del server web che ospita la pagina web.

- **Checking.faw**
  è il file che contiene un codice di controllo che permette di verificare se i file Acquisition.txt e Acquisition.xml non sono stati alterati.

- **Code.htm**
  è un file html che contiene tutto il codice HTML della pagina web.

- **CodeFrame{nomeframe}.htm**
  sono file che contengono il codice HTML del frame {nomeframe} se presente.

- **Headers.txt**
  è un file di testo che contiene gli headers inviati al browser dalla pagina web.

- **hosts**
  è la copia del file hosts di windows al momento dell'acquisizione della pagina Web.

- **Image.png**
  è il file che contiene l'immagine della pagina web delimitata dalla Gold Box in formato png a 24bit.

- **Image{numero}.png**
  sono file immagine con i ritagli dell'immagine completa della pagina Web acquisita con aspect-ratio 1,41 adatte ad essere stampate a pagina intera su fogli A4.

- **screenCapture.wmv**
  è il file video acquisito da VLC con la cattura dell'intero schermo del computer dall'inizio dell'acquisizione fino alla fine.

- **SystemLogEvents.txt**
  è il file in cui vengono registrati tutti gli eventi di windows avvenuti durante l'acquisizione della pagina Web.

- **Wireshark_{mac-address-network-interface}.pcap**
  è il file acquisito da Wireshark con il traffico di rete avvenuto durante l'acquisizione della pagina Web.

- **Cartella Objects**
  la cartella contiene tutti gli elementi della pagina Web acquisiti (immagini, documenti, script, ecc.) e numerati progressivamente con il formato [nnnnn]filename.ext.

- **Cartella ImagesA4**
  la cartella contiene il file Image.png (screenshot della pagina web) ritagliata in più immagini con un rapporto base/altezza del formato A4. Queste immagini sono l'ideale per essere inserite in report che devono essere stampati.

Ogni acquisizione viene inserita in una sotto cartella numerata sequenzialmente (esempio: 00001, 00002, 00003, … 0000n) della cartella padre con nome del Case ID scelta dall'utente all'avvio del programma.

ATTENZIONE: queste cartelle non devono essere rinominate altrimenti il software non può creare le successive cartelle e verrà generato un errore.

Per certificare ulteriormente la data e l'ora dell'acquisizione della pagina web si può firmare digitalmente il solo file Acquisition.txt oppure il file Acquisition.xml ricordandosi di apporvi anche una marca temporale che certifica la data dell'acquisizione; in alternativa è possibile anche creare un archivio compresso di tutta la cartella dell'acquisizione e firmare digitalmente quest'ultimo.

Salvataggio dei dati dell'acquisizione su server FAW

Le acquisizioni eseguite da FAW possono essere inviate al server di conservazione di FAW; se si vuole utilizzare questa funzione la si deve attivare dal menu Configuration > Preferences > Pro Acquisition attivando la casella "Upload acquisition on FAW Server".

In questo modo, al termine dell'acquisizione, FAW chiede se si vuole salvare i dati dell'acquisizione sul server FAW; i dati che verranno salvati sono i seguenti: checking code, data inizio e fine acquisizione, URL acquisito e l'indirizzo IP del client che ha eseguito l'acquisizione.

Se l'utente acconsente all'invio di questi dati gli stessi saranno memorizzati nel database del server FAW e saranno disponibili per eseguire verifiche on-line dell'integrità dell'acquisizione.

I dati sul server di FAW vengono conservati per 3 anni. Se l'utente vuole prolungare la conservazione degli stessi deve acquistare un'estensione della conservazione scrivendo a support@fawproject.com almeno 10 giorni prima della scadenza.

Verifica integrità dell'acquisizione

È possibile verificare se i file Acquisition.txt e Acquisition.xml non sono stati alterati mediante la funzione di "Acquisition checking" disponibile nel menu "Checking".

Verifica dell'acquisizione in locale

Nel menù Checking, cliccando su "Acquisition checking" si apre la finestra "Cerca cartella" nella quale si dovrà selezionare la cartella in cui è contenuta l'acquisizione che si vuole verificare; cliccando quindi su [OK] il programma verifica l'integrità dei due file Acquisition.txt e Acquisition.xml e mostra il risultato della verifica.

La funzione di verifica utilizza un algoritmo proprietario che alla fine dell'acquisizione della pagina Web genera un codice di verifica che viene salvato nel file Checking.faw; tale file deve essere presente nella stessa cartella insieme a Acquisition.txt e Acquisition.xml quando si deve procedere alla verifica.

Verifica dell'acquisizione on line

Se i dati dell'acquisizione sono stati salvati anche sul server FAW, è possibile eseguire una verifica dell'integrità dei files Acquisition.txt e Acquisition.xml mediante confronto con i dati memorizzati nel database di FAW.

Per far ciò è sufficiente aprire il menu Checking e cliccare sulla voce "Acquisition checking on line" verrà visualizzata la pagina di verifica nel browser predefinito.

La pagina di verifica utilizza il protocollo https per garantire la sicurezza dei dati forniti dall'utente; in questa pagina si dovranno caricare i due file Acquisition.txt e Acquisition.xml da verificare, e quindi cliccare il pulsante [Check]; il programma verifica l'integrità di entrambi i files certificando se essi non sono stati alterati. La stessa pagina, qualora la verifica fosse corretta, mostrerà i dati della relativa acquisizione salvati nel database del server FAW.

Questa procedura è un ulteriore strumento per il consulente tecnico per verificare l'integrità delle acquisizioni eseguite con il software FAW.

Verifica dei dati di un'acquisizione sul server FAW

È possibile verificare su sul server FAW sono presenti i dati di una particolare acquisizione; per far ciò, dal menu Checking, si clicca sulla voce "Verify the presence of acquisition on FAW server"; verrà visualizzata la pagina di ricerca nel browser predefinito.

In questa pagina è sufficiente caricare il file Checking.faw di una acquisizione per verificare se i dati di tale acquisizione sono stati salvati nel database del server FAW.

Se il checking code contenuto nel file Checking.faw è presente nel database verranno mostrati tutti i relativi dati dell'acquisizione.

Invio dell'acquisizione tramite e-mail

Il programma permette di inviare automaticamente l'acquisizione appena effettuata ad una casella e-mail; per evitare l'invio di allegati troppo pesanti vengono spediti solamente i file Acquisition.txt, Acquisition.xml e Checking.faw. L'invio automatico tramite e-mail permette di inviare l'acquisizione anche ad una casella di posta certificata PEC (mediante il proprio client di posta) e quindi di certificare temporalmente la data di acquisizione.

Dal menu Configuration > Preferences selezionare il tab "Pro-Email" – Fig. 8.

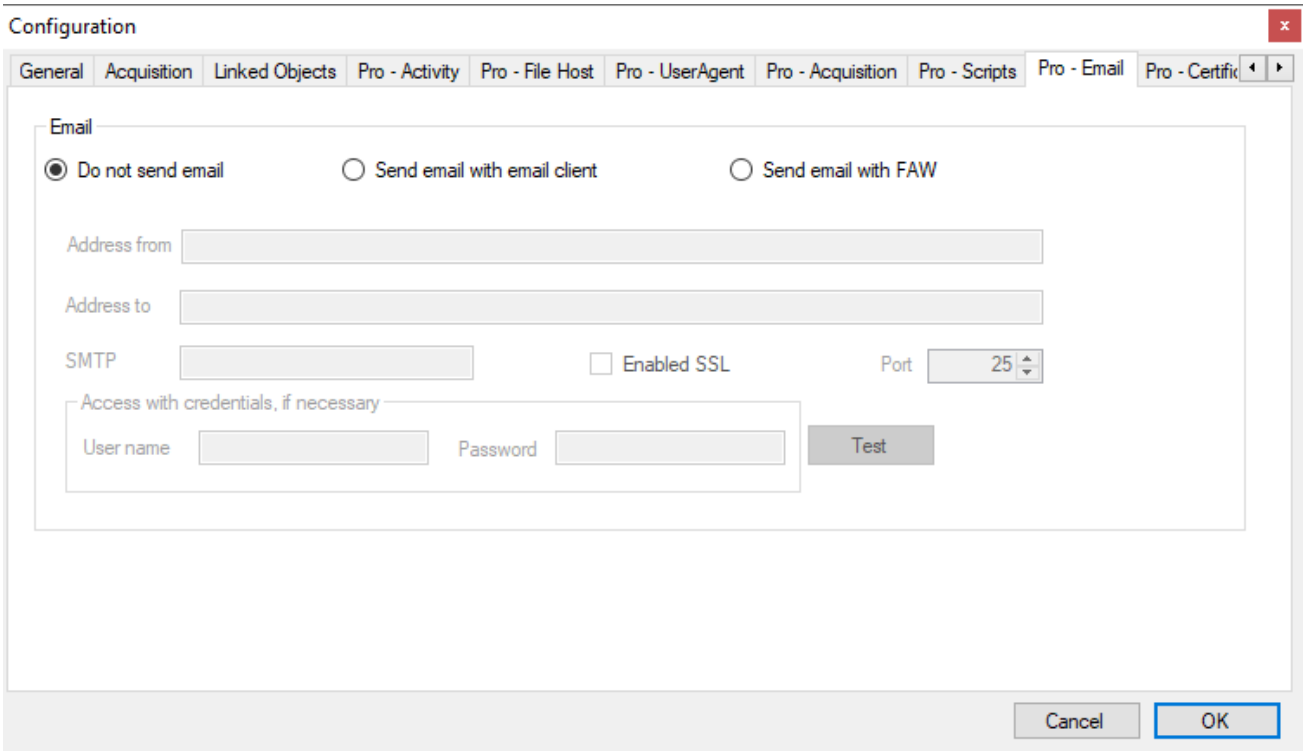


Fig. 8

Le opzioni disponibili sono:

- **Do not send email**
  Disattiva l'invio della e-mail

- **Send email with email client**

  Invia la e-mail al termine dell'acquisizione utilizzando il proprio client di posta elettronica predefinito

- **Send email with FAW**

  Il programma invia direttamente una e-mail al termine dell'acquisizione, in questo caso è necessario inserire i dati del proprio account di posta elettronica e l'indirizzo del destinatario

  Se la mail deve essere inviata ad un indirizzo di posta certificata PEC è necessario utilizzare l'invio tramite il proprio client di posta su cui è configurato l'account PEC.

Utilizzo del tool FAW STOP

FAW STOP è il tool che permette di effettuare l'acquisizione di due screenshot della stessa pagina in momenti diversi, mentendo attiva la registrazione dello screencast e dello sniffer di rete. Questo tool si presta per acquisizione di pagine web che contengono elementi multimediali (audio e video) o streaming.

La prima acquisizione viene eseguita prima di riprodurre l'elemento multimediale, mentre la seconda al termine della riproduzione; l'elemento multimediale viene acquisito nella registrazione dello screencast (assicurarsi che in Configuration > Preferences > Pro Activity sia spuntata la casella "Active video acquisition").

La differenza principale con il tool FAW è la presenza di due pulsanti, anziché uno, per effettuare la prima e la seconda acquisizione (Fig. 9).

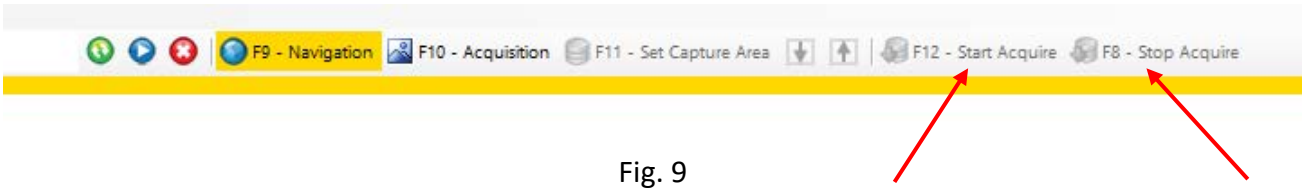


Fig. 9

Il pulsante denominato [Start Acquire] avvia la prima acquisizione – deve quindi essere premuto prima di eseguire l'elemento multimediale, mentre il pulsante denominato [Stop Acquire] deve essere premuto dopo che è terminata la riproduzione dell'elemento multimediale.

I passi corretti, quindi, per acquisire una pagina con un elemento multimediale sono i seguenti:

1. In modalità Navigazione raggiungere la pagina che contiene l'elemento multimediale da acquisire.
2. Premere il pulsante [Start Acquire] e attendere il completamento della prima acquisizione.
3. Avviare la riproduzione dell'elemento multimediale.
4. Al termine della riproduzione dell'elemento multimediale premere il pulsante [Stop Acquire].

Nella cartella del Caso troverete la sotto cartella numerica in cui saranno presenti:

- una cartella denominata START in cui saranno presenti tutti gli elementi della prima acquisizione;
- una cartella STOP in cui saranno presenti tutti gli elementi della seconda acquisizione;
- il file dello screencast tra le due acquisizioni;
- il file dello sniffer tra le due acquisizioni.

Utilizzo del tool FAW TIME

FAW STOP è il tool che permette di effettuare acquisizioni della stessa pagina web in modo schedulato.

Il funzionamento è identico al tool FAW a parte la presenza di una casella di testo in cui inserire il tempo (espresso in secondi) della schedulazione - Fig. 10.

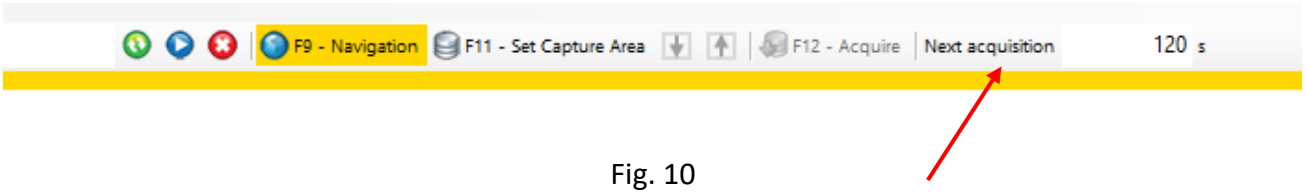


Fig. 10

I passi corretti, quindi, per acquisire una pagina web in modo schedulato sono i seguenti:

1. In modalità Navigazione raggiungere la pagina web che si deve acquisire.
2. Inserire nella casella di testo “Next acquisition” i secondi dopo i quali l’acquisizione deve essere ripetuta.
3. Selezionare l’area di cattura regolando la Gold Box.
4. Premere il pulsante [Acquire] e attendere il completamento della prima acquisizione.
5. Le successive acquisizioni verranno effettuate in automatico ogni periodo di tempo indicato nella casella di testo “Next acquisition”
6. Per terminare le acquisizioni chiudere il programma cliccando sull’icona [X] nella barra del titolo.

Nella cartella del Caso troverete la sotto cartella numerica in cui saranno presenti diverse sottocartelle ognuna delle quali ha come nome la data e l’ora dell’acquisizione.

Utilizzo del tool FAW TOR

FAW TOR è il tool che permette di effettuare acquisizioni di pagine web dalla rete TOR.

Il funzionamento è identico al tool FAW a parte, unica differenza è che viene aperta una sessione sulla rete TOR.

L'avvio del tool FAW TOR può richiedere più tempo di FAW perché è necessario attendere che venga stabilita la connessione con la rete TOR; la prima pagina che mostra FAW TOR è quella di test che indica all'utente se è riuscita la connessione sulla rete TOR – Fig. 11.

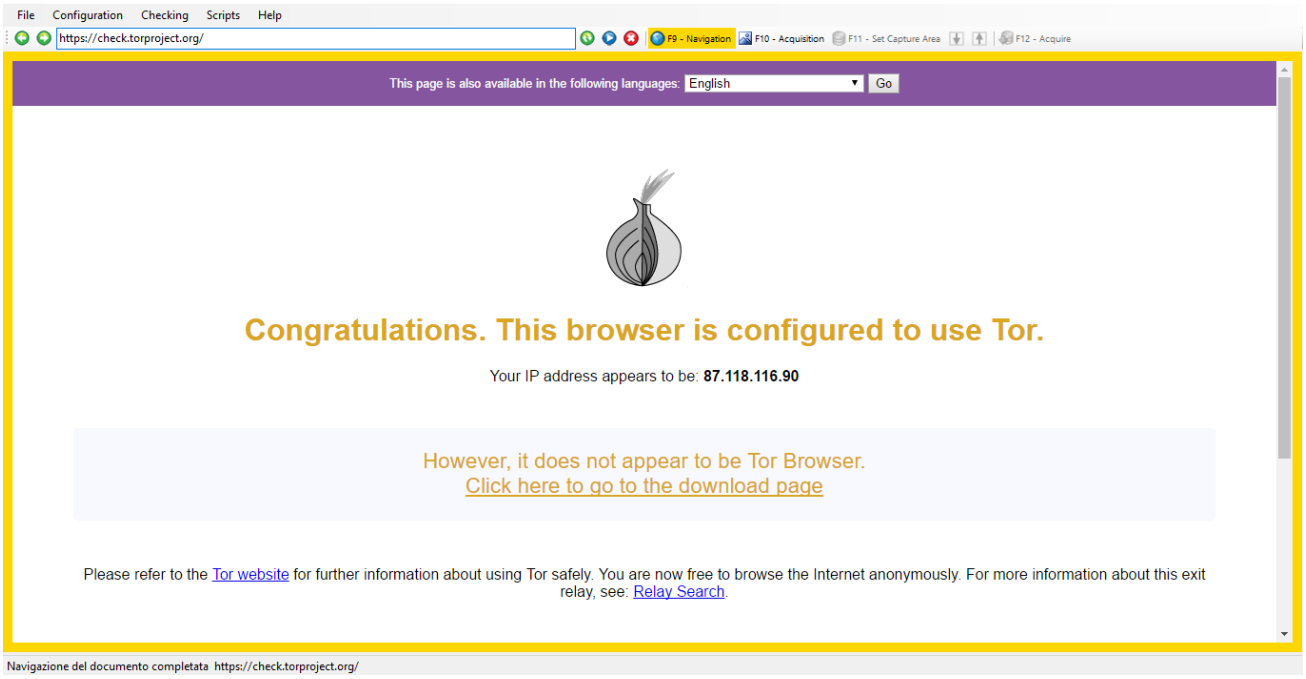


Fig. 11

Anche la chiusura del tool richiede più tempo di FAW perché deve disconnettersi dalla rete TOR, chiudere il proxy e riportare la configurazione di rete del computer in modo standard.

Utilizzo del tool FAW BOT

FAW BOT è un crawler che permette di cercare tutti gli URL delle pagine collegate alla pagina iniziale da cui viene iniziata la ricerca. La caratteristica più interessante di questo tool è la possibilità di cercare pagine e informazioni in siti web protetti da credenziali (esempio: Facebook, Linkedin, ecc…).

Nella barra superiore di FAW BOT (Fig. 11) sono presenti i seguenti pulsanti e opzioni:

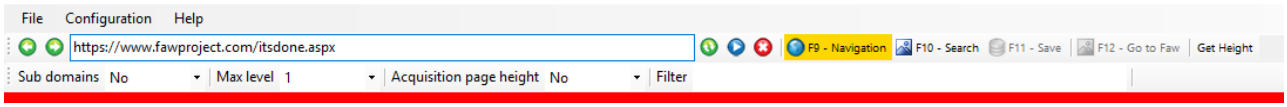


Fig. 11

- **[Navigation]**
  Permette di navigare come un normale browser
- **[Search]**
  Inizia la ricerca del URL
- **[Save]**
  Salva l'elenco degli URL trovati in un file
- **[Go to FAW]**
  Esporta l'elenco dei URL trovati direttamente nel tool FAW MULTI per l'acquisizione automatica
- **[Get Height]**
  Tenta di ottenere l'altezza totale della pagina web visualizzata

Oltre a questi cinque pulsanti sono presenti anche delle opzioni:

- **"Sub Domains"**
  Scegliere "yes" se si vuole che la ricerca comprenda anche i sotto domini, altrimenti lasciare "no".
- **"Max Level"**
  Permette di scegliere la profondità (livelli) in cui deve essere eseguita la ricerca.
- **"Acquisition page height"**
  Se viene selezionato "auto" il tool cerca di trovare l'altezza totale della pagina visualizzata (attenzione l'utilizzo di questa funzionalità potrebbe rallentare di molto la ricerca).
- **"Filter"**
  È una casella di testo che può essere utilizzata per filtrare i risultati utilizzando le regular

expression. A esempio se si vogliono solo le pagine che contengono la parola “business” basterà scrivere nella casella Filter: business; se si vogliono solo le pagine che contengono un qualsiasi indirizzo e-mail basterà scrivere nella casella Filter: ^[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9](?:[a-zA-Z0-9-]{0,61}[a-zA-Z0-9])?(?:\.[a-zA-Z0-9](?:[a-zA-Z0-9-]{0,61}[a-zA-Z0-9])?)*$

I passi corretti, quindi, per utilizzare la ricerca con il tool FAW BOT sono i seguenti:

1. In modalità Navigazione raggiungere la pagina da cui deve partire la ricerca.

2. Impostare le opzioni di ricerca: sotto domini, livelli, altezza pagina e filtro.

3. Premere il pulsante [Search]

4. Al termine della ricerca cliccare sul pulsante [Save], i risultati della ricerca verranno salvati nella cartella del Caso con il nome ResultsBOT001.xml, in caso di più ricerche i file si chiameranno ResultsBOT002.xml, ResultsBOT003.xml … ecc.

5. A questo punto se si vuole iniziare l’acquisizione dei siti web si deve cliccare il pulsante [Go to FAW], in questo modo FAW BOT si chiudi e viene aperto il tool FAW MULTI per l’acquisizione automatica delle pagine trovate.

Struttura del file ResultsBOT001.xml

Qui di seguito è mostrato un esempio del contenuto del file xml con i risultati della ricerca:

```
<?xml version="1.0" encoding="UTF-8"?>
<CrawlerResults>
  <CrawlerResult>
    <Height>0</Height>
    <Url>https://www.testurl.com/</Url>
    <TimeSecondsFrom>0</TimeSecondsFrom>
    <TimeSecondsTo>0</TimeSecondsTo>
  </CrawlerResult>
  <CrawlerResult>
    <Height>1550</Height>
    <Url>https://www.testurl.com/contacts/</Url>
    <TimeSecondsFrom>10</TimeSecondsFrom>
    <TimeSecondsTo>10</TimeSecondsTo>
  </CrawlerResult>
  <CrawlerResult>
    <Height>9000</Height>
    <Url>https://www.testurl.com/feed/</Url>
    <TimeSecondsFrom>30</TimeSecondsFrom>
    <TimeSecondsTo>30</TimeSecondsTo>
  </CrawlerResult>
  <CrawlerResult>
    <Height>748</Height>
    <Url>https://www.testurl.com/comments/video/a1s4frk/</Url>
    <TimeSecondsFrom>15</TimeSecondsFrom>
    <TimeSecondsTo>220</TimeSecondsTo>
  </CrawlerResult>
</CrawlerResults>
```

Utilizzo del tool FAW MULTI

FAW MULTI è un tool che permette l'acquisizione automatica di un elenco di pagine web.

La barra superiore (Fig. 13) contiene i seguenti elementi:

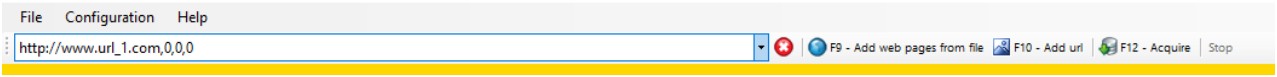


Fig. 13

- **Menu a discesa**
  mostra l'elenco delle pagine web che devono essere acquisite.
- **Pulsante [Add web pages from file]**
  permette di importare un elenco di pagine web precedentemente salvate in un file xml.
- **Pulsante [Add URL]**
  permette di aggiungere manualmente degli URL all'elenco delle pagine da acquisire.
- **Pulsante [Acquire]**
  Inizia l'acquisizione automatica delle pagine contenute nell'elenco visibile nel menu a discesa.
- **Pulsante [Stop]**
  Ferma l'acquisizione.

FAW MULTI può acquisire in automatico pagine web impostando anche l'altezza della Gold Box, un tempo di attesa iniziale, ed eventualmente eseguire due acquisizioni della stessa pagina ad un determinato intervallo (con le stesse modalità del tool FAW STOP).

Per automatizzare queste funzioni oltre all'URL della pagina da acquisire deve essere indicato anche l'altezza della pagina web da acquisire e due intervalli di tempo espressi in secondi.

Questi tre parametri sono così impostati:

```
https://www.testurl.com/contacts/,{p1},{p2},{p3}
```

Dove:

p1 = è l'altezza della pagina espressa in pixel

p2 = è il tempo dopo il quale inizia la prima acquisizione espresso in secondi

p3 = è il tempo dopo il quale inizia la seconda acquisizione espresso in secondi

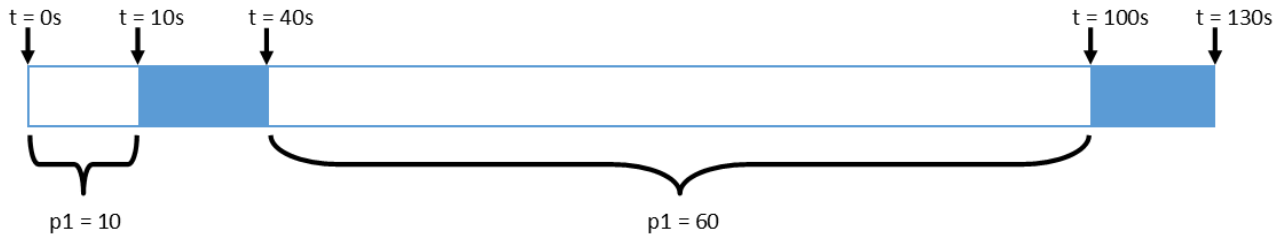
Se i parametri p2 e p3 sono uguali verrà effettuata una sola acquisizione.

Se non viene indicato alcun parametro l'acquisizione della pagina web viene effettuata con l'altezza di default del browser e immediatamente al caricamento della stessa.

Ricordarsi che per eseguire una doppia acquisizione il tempo del parametro p3 deve essere sempre superiore al tempo del parametro p2 ed è consigliabile avere una differenza di almeno 30" (tempo necessario al software per acquisire tutti gli elementi della pagina prima di passare alla seconda acquisizione).

Il primo parametro di tempo p1 è riferito al termine di caricamento della pagina web, mentre il secondo parametro p2 è il tempo che deve trascorrere dal termine della prima acquisizione prima di iniziare la seconda.

Lo schema seguente mostra il funzionamento dei due parametri p1 e p2.



Nell'esempio mostrato qui sopra p1 è stato impostato a 10 secondi, mentre p2 è impostato a 60 secondi. Il workflow di FAW MULTI è il seguente: dopo l'attesa di 10 secondi viene avviata la prima acquisizione che impiega 30 secondi, al termine dell'acquisizione inizia la seconda attesa di 60 secondi alla fine della quale viene eseguita la seconda acquisizione.

Da questo schema si può dunque capire che il tempo indicato dal parametro p2 inizia dal termine della prima acquisizione.

Se i parametri p1, p2 e p3 non vengono indicati, FAW MULTI li imposta a zero, in questo modo eseguirà l'acquisizione con l'altezza della Gold Box predefinita e immediatamente al termine di caricamento della pagina web.

L'inserimento degli URL da acquisire si può fare in due modi: inserendoli manualmente o importando il file xml generato dal tool FAW BOT.

Inserimento manuale degli URL da acquisire

Per inserire una lista di URL da acquisire in modo automatico cliccate sul pulsante [Add URL], si aprirà una finestra – Fig. 14 – contenente un campo testo dove è possibile inserire tutti gli URL da acquisire, uno per ogni riga.

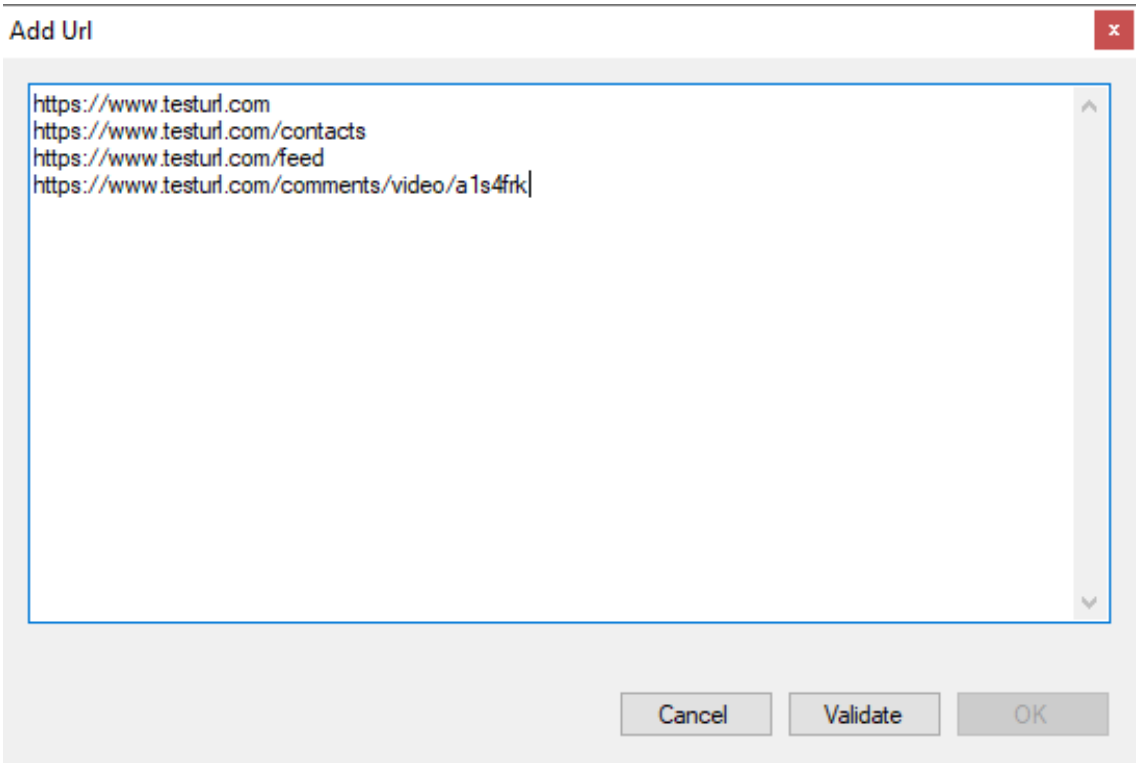


Fig. 14

Cliccate quindi sul pulsante [Validate], gli URL verranno verificati e se sono corretti si attiverà il pulsante [OK].

Se viene inserito un URL senza indicare il protocollo http o https, FAW MULTI lo completerà mettendoci davanti http:// - se avete la necessità di acquisire pagine con protocollo https dovete inserire un URL preceduto da https://.

A questo punto cliccando sul pulsante [OK] la lista degli URL verrà importata nel menù a discesa delle pagine che devono essere acquisite. Come si vede dalla Fig. 15 per ogni URL sono stati aggiunti i tre parametri descritti in precedenza.

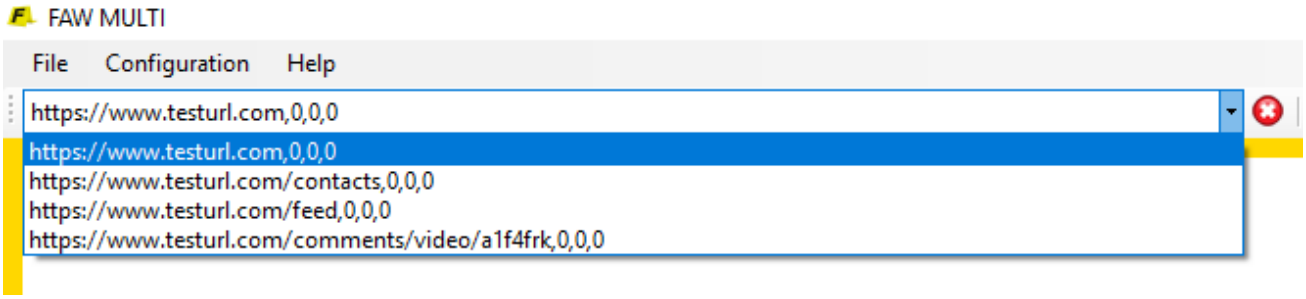


Fig. 15

Ovviamente non avendo indicato i parametri p1, p2 e p3 il software di default li mette a zero.

Inserimento elenco URL da file XML

L'elenco degli URL da acquisire si può anche importare da un file XML cliccando sul pulsante [Add web pages from file].

Il file XML deve rispettare la struttura di quello generato dal tool FAW BOT; qui di seguito si riporta un esempio:

```
<?xml version="1.0" encoding="UTF-8"?>
<CrawlerResults>

  <CrawlerResult>
    <Height>Altezza Gold Box (pixel)</Height>
    <Url>URL da acquisire<Url>
    <TimeSecondsFrom>parametro p1 (secondi)</TimeSecondsFrom>
    <TimeSecondsTo> parametro p2 (secondi)</TimeSecondsTo>
  </CrawlerResult>

  <CrawlerResult>
    <Height>Altezza Gold Box (pixel)</Height>
    <Url>URL da acquisire<Url>
    <TimeSecondsFrom>parametro p1 (secondi)</TimeSecondsFrom>
    <TimeSecondsTo> parametro p2 (secondi)</TimeSecondsTo>
  </CrawlerResult>

</CrawlerResults>
```

Avvio delle acquisizioni

Una volta caricata la lista degli URL da acquisire è sufficiente cliccare sul pulsante [Acquire] per dare inizio alle acquisizioni automatiche.

Se per qualsiasi motivi è necessario fermare il processo di acquisizione si può premere il pulsante [Stop].

Utilizzo del tool FAW FTP

FAW FTP è un tool che permette di scaricare un intero sito web tramite protocollo FTP senza alterare data e ore dei file, così come sono sul server web.

Pe eseguire l'acquisizione è sufficiente compilare tutti i campi per autenticarsi sul server web con il protocollo FTP: "Host", "Port", "Username", "Password", "Remote folder" e "Date Time format".

L'ultimo parametro "Date Time format" specifica il formato della data e dell'ora utilizzato sul server. Lasciando questo campo vuoto FAW FTP ne determina automaticamente il formato corretto. In rari casi è possibile che il riconoscimento automatico non sia possibile, in questo caso si può indicare manualmente come è strutturata data e ora sul server web utilizzando questa sintassi:

d = giorno con una o due cifre

dd = giorno con sempre due cifre

M = mese con una o due cifre

MM = mese con due cifre

yy = anno con due cifre

yyyy = anno con quattro cifre

HH = ore con due cifre

mm = minuti con due cifre

ss = secondi con due cifre

tt = utilizza AM/PM

si deve inoltre indicare il separatore utilizzato per la data e quello per le ore.

Un esempio di un Date Time format italiano è:

dd/MM/yyyy HH:mm:ss

In questo caso il separatore della data è lo slash “/”, mentre per l’ora sono i due punti “:”, la data è separata dall’ora da uno spazio.

Per capire il formato della data e dell’ora utilizzati sul server da cui si vuole eseguire l’acquisizione è sufficiente collegarsi con un client FTP e osservare il formato di data e ora e quindi indicarlo in FAW FTP.

Una volta completati tutti i campi è sufficiente cliccare sul pulsante [Acquire] per iniziare l’acquisizione di tutti i file contenuti nella cartella remota del server web.

Nel box “Acquisition status” verranno mostrate le operazioni eseguite dal software.

Utilizzo del tool FAW REPORT

FAW REPORT è il tool che permette di generare un report di tutte le acquisizioni eseguite all'interno dello stesso Case ID.

Nella finestra principale di FAW REPORT appaiono tutte le acquisizioni del caso aperto - Fig. 16 - da qui è possibile spuntare solo quelle che devono essere incluse nel report.

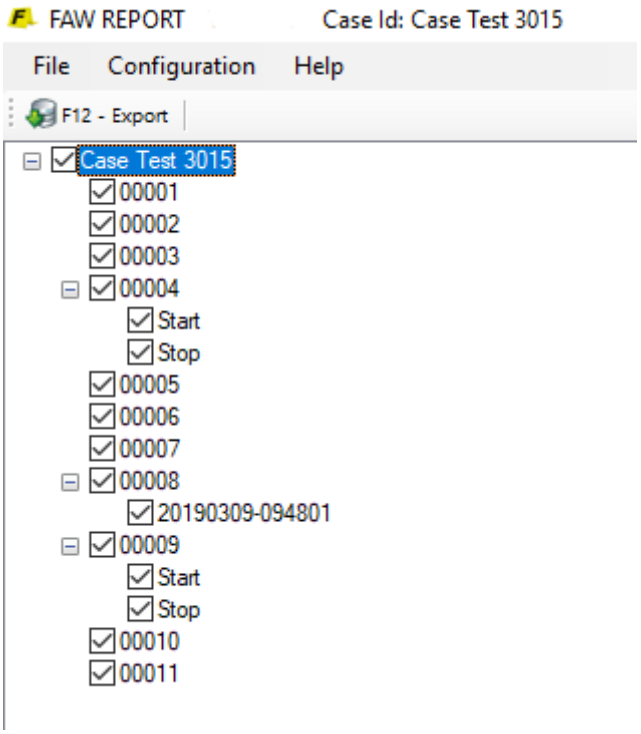


Fig. 16

Una volta scelte le acquisizioni da importare nel report è sufficiente cliccare sul pulsante [Export] per generare il report.

La generazione del report si basa su un modello di documento Word che si trova nella cartella "Template" all'interno della cartella di installazione di FAW; il file si chiama FAW_REPORT.docx.

Questo file può essere personalizzato dall'utente come meglio crede; i tag per l'inserimento degli elementi delle acquisizioni sono i seguenti:

<FAWCASE> Scrive il nome del caso.

<FAWDETECTIVE> Scrive il nome dell'investigatore che ha aperto il caso.

<FAWVERSION> Scrive il numero della versione di FAW che ha generato il report.

<FAWTEXTACQUISITIONS> Scrive tutti i file Acquisition.txt di tutte le acquisizioni selezionate.

<FAWIMAGESACQUISITIONS> Scrive tutti i file imagine contenuti nella cartella ImagesA4 di ogni acquisizione di tutte le acquisizioni selezionate.