

# Acquisizione forense pagine web

*Come agire in caso di diffamazione sul web*

**Autore: Davide Grimaldi**

---

Contatti:  
davidegrimaldi92@gmail.com

---

# Contenuti

Introduzione	1
1. Reato di diffamazione	
2. Diffamazione sul web	
Acquisizione forense	3
1. Acquisizione forense pagine web: caratteristiche	
Software per l'acquisizione forense: FAW	4
1. Breve storia	
2. Storico caratteristiche generali	
3. Utilizzo	
4. Esempio: acquisizione profilo LinkedIn	
5. Interpretazione e trattamento dati acquisiti	
Riferimenti	14

## Introduzione

---

### Contenuto e scopo

Le procedure descritte, in questa trattazione a carattere generale, riguardano il caso di reato di diffamazione ma possono essere estese con le dovute accortezze anche ad altri reati che necessitano la raccolta di prove sul web, ad esempio violazione di copyright. Ci si rivolge ad un pubblico di non addetti ai lavori e non si entra in modo approfondito nei dettagli tecnici.

### Reato di diffamazione

La diffamazione è un reato previsto e punito dall'art. 595 c.p. e consiste nell'offesa all'altrui reputazione fatta comunicando con più persone:

“Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a mille trentadue euro.

[...]

Se l'offesa è recata col mezzo della stampa [57-58bis] **o con qualsiasi altro mezzo di pubblicità**, ovvero in atto pubblico [2699], la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a cinquecento sedici euro.”

I presupposti del reato sono i seguenti:

- **L'assenza dell'offeso**, consistente nell'impossibilità che la persona offesa percepisca direttamente l'addebito diffamatorio. L'impossibilità di difendersi determina infatti una maggiore potenzialità offensiva rispetto alla mera ingiuria (ad oggi comunque depenalizzata).
- **L'offesa alla reputazione**, intendendosi la possibilità che l'uso di parole diffamatorie possano ledere la reputazione dell'offeso.
- **La presenza di almeno due persone** in grado di percepire le parole diffamatorie (esclusi il soggetto agente e la persona offesa). La giurisprudenza ritiene configurato il delitto in esame anche qualora l'offesa sia comunicata ad una persona sola, affinché questa, però, la comunichi ad altre.

Importante da notare nell'articolo la previsione di un “qualsiasi altro mezzo di pubblicità”: esso è estendibile all'utilizzo di social networks e pagine web che permettano una, anche solo potenziale, diffusione ad un numero indeterminato di persone del messaggio diffamatorio.

## Diffamazione sul web

La crescita esponenziale della opportunità, tramite internet, di comunicazione fra gli individui ha aumentato la possibilità di trasmettere proprie opinioni e pensieri:

- Con maggiore velocità
- Semplicità: chiunque è in grado di postare un contenuto su internet
- Possibilità di raggiungere un pubblico di dimensioni indefinite
- Diffusione incontrollabile, in quanto si tratta di algoritmi (molto complicati) che dettano le dinamiche di propagazione

Questo ha comportato una diffusione senza precedenti di possibili informazioni false su fatti e persone, citando Umberto Eco: “I social media danno diritto di parola a legioni di imbecilli che prima parlavano solo al bar dopo un bicchiere di vino, senza danneggiare la collettività.

Venivano subito messi a tacere, mentre ora hanno lo stesso diritto di parola di un Premio Nobel. È l'invasione degli imbecilli.”

La

diffamazione via web o tramite piattaforma social è diventata ormai una pratica diffusa; la cassazione ha riconosciuto espressamente la possibilità che il reato di diffamazione sia commesso a mezzo internet, ad esempio tramite Facebook:

### **Cass. pen. n. 24431/2015**

“La diffusione di un messaggio diffamatorio attraverso l'uso di una bacheca "facebook" integra un'ipotesi di diffamazione aggravata ai sensi dell'art. 595, comma terzo, c.p., poiché trattasi di condotta potenzialmente capace di raggiungere un numero indeterminato o comunque quantitativamente apprezzabile di persone.”

Si configura quindi la necessità di acquisire in modo sicuro e certificato le informazioni “intangibili” nel web riguardanti il suddetto reato.

## Acquisizione forense

### Acquisizione forense pagine web: caratteristiche

La caratteristica principale di una acquisizione forense è la garanzia della autenticità delle informazioni raccolte; essa è garantita utilizzando metodo scientifico e strumentazione adatta. La semplice stampa cartacea, la fotografia dello schermo o screenshot hanno scarso valore legale: esse infatti possono essere contestate dalla controparte perché facilmente falsificabili.

*"La copia di una pagina web su supporto cartaceo ha valore probatorio solo se raccolta con le dovute garanzie. Per la rispondenza all'originale e la riferibilità a un momento ben individuato - Le informazioni tratte da una rete telematica sono per loro natura volatili e suscettibili di continua trasformazione. Va escluso che costituisca documento utile ai fini probatori una copia di pagina web su supporto cartaceo che non risulti essere stata raccolta con garanzia di rispondenza all'originale e di riferibilità a un ben individuato momento" (Cassazione Sezione Lavoro n. 2912 del 18 febbraio 2004, Pres. Mattone, Rel. Spanò).*

La copia e l'acquisizione forense di una prova presente in Internet è sempre più spesso fondamentale nella risoluzione di un contenzioso in quanto "cristallizza" con metodi forensi il contenuto dell'informazione permettendo, ove si renda necessario, chiarire il quadro indiziario. Proprio per questo soprattutto nell'ultimo decennio sono nati innumerevoli software/servizi per l'acquisizione forense di contenuti sul web. La maggior parte dei software sul mercato funziona effettuando l'acquisizione in modalità simile alla semplice navigazione in Internet. Tramite il pc dell'utente viene reso disponibile un "browser virtuale", con il quale è possibile accedere a qualunque sito web pubblico o privato. Tutta la navigazione viene registrata ed è possibile archiviare qualunque materiale presente in rete. Tutto ciò che viene scaricato - compreso il video dell'intera navigazione - sarà automaticamente reso disponibile all'interno di un archivio, dopo il termine dell'acquisizione oltre ai metadati necessari (filerobots.txt, certificati SSL, sitemap, metadati RSS, filmato dell'acquisizione forense, indirizzi IP, record DNS ecc.).

Nel seguito verrà discusso l'utilizzo, con relativo esempio, del software FAW: Forensics Acquisition of Websites.

## Software per l'acquisizione: FAW

### Breve storia

Sviluppato da due italiani nel 2013, FAW: "è stato il primo software in grado di acquisire in modo certificato anche pagine protette da credenziali, come Facebook, incluse gallerie di foto, chat, aree riservate, permettendo la verifica delle acquisizioni da parte di terzi e l'utilizzo in Tribunale in procedimenti civili e penali" (guida FAW). Nasce come software forense per gli addetti ai lavori, ma la sua semplicità permette il suo impiego anche ai non esperti. Dal 2013 ad oggi si sono susseguite varie versioni con miglioramenti tecnici e applicativi sostanziali: l'ultima versione FAW 7 è apprezzata in Italia ed all'estero, viene adottata come primo *tool* dalla polizia polacca ed è presentata in congressi e conferenze internazionali del settore.

### Storico delle caratteristiche generali

A partire dalla versione 2.0 è dotato di un nuovo algoritmo che permette di verificare se l'acquisizione sia stata alterata o meno. FAW acquisisce tutti gli oggetti collegati ad una pagina web: immagini, archivi, documenti, eseguibili, script. Dal 2014 è disponibile l'integrazione con Wireshark che permette di registrare tutto il traffico di rete in uscita ed entrata durante una acquisizione allo scopo di garantirne una maggiore autenticità (è prova di non alterazione). Il software effettua la registrazione dello schermo durante tutte le operazioni di acquisizione ed è in grado di certificarla. Dalla versione 4.0 è presente l'utilissima funzionalità di salvare copia delle acquisizioni fatte su server remoto, per utilizzarle al fine eseguirne la validazione, aumentandone ulteriormente l'affidabilità. È presente anche la possibilità di mandare in automatico una email (preferibilmente PEC) con le caratteristiche dell'acquisizione appena terminata al fine di validare ulteriormente ora e data. Esiste la possibilità di utilizzare FAW direttamente da macchina virtuale tramite Virtual Box, è presente un pacchetto VirtualBox con FAW e Wireshark preinstallati e già configurati, tramite il quale viene garantito un ambiente pulito, certificato e privo di qualsiasi tipo di software malevolo. Con la versione 7.0 sono stati aggiunti numerosi strumenti:

- FAW TOR: acquisizione pagine sul Darkweb
- FAW TIME: schedulazione acquisizione
- FAW BOT: ricerca di tutte le pagine web collegate ad un sito web
- FAW MULTI: consente di catturare contemporaneamente più pagine web
- FAW REPORT: creazione report dettagliati su tutte le attività svolte

## Utilizzo

Si vedranno adesso le operazioni necessarie per eseguire un'acquisizione utilizzando FAW.

### 1) Avvio

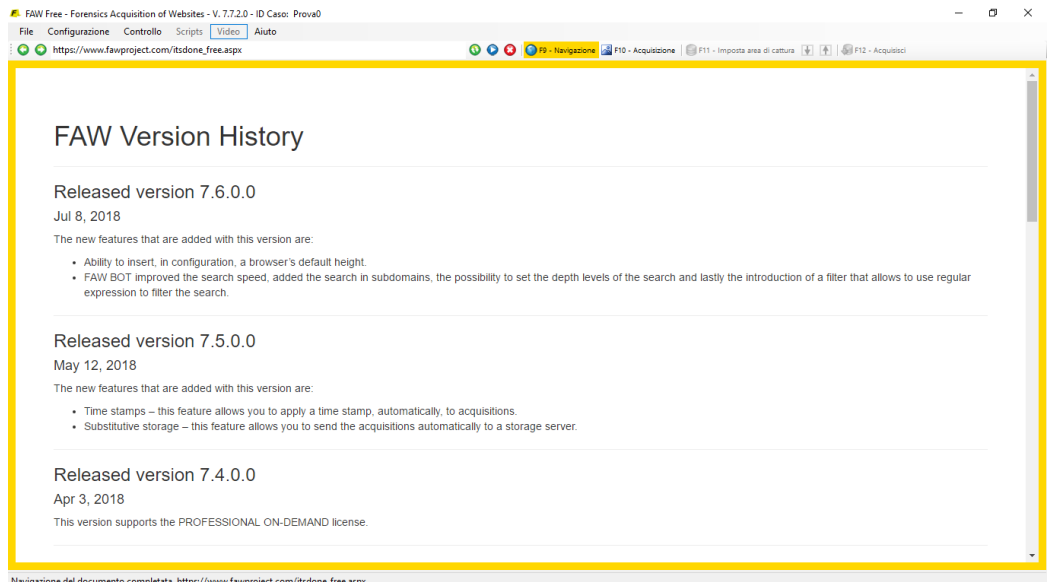


Figura 1

In avvio si presenta una finestra(**Fig.1**) con due campi. Il campo “investigatore”, per l'identificativo di chi svolge le attività investigative, è un campo opzionale e può anche essere lasciato vuoto. Il secondo campo, obbligatorio, è quello dell'identificativo del caso: esso può contenere qualsiasi sequenza alfanumerica di caratteri; questo id sarà il nome della cartella in cui FAW inserirà tutti i file riguardanti le acquisizioni che, se facenti parte dello stesso caso saranno segnate da un numero progressivo. Ad ogni avvio FAW cancella la propria cache dei file temporanei e dei cookie.

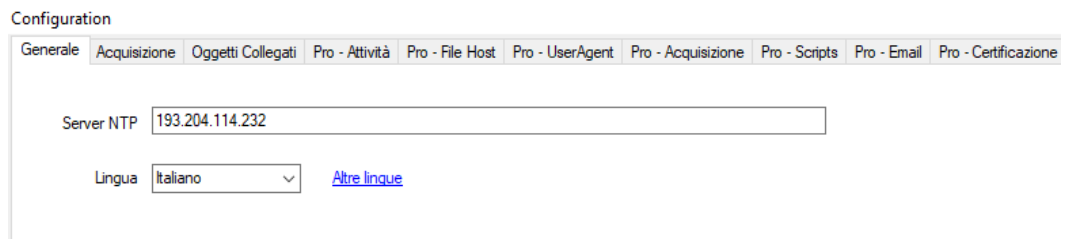
## 2) Opzioni e configurazione

Figura 2



Dopo aver cliccato su “OK”, si presenterà una schermata(**Fig.2**) molto simile a quella di un browser convenzionale. La pagina iniziale di default è quella in cui vengono fornite le ultime notizie ed gli aggiornamenti sul software. Dalla barra dei menu, alla voce “configurazioni” si può accedere alle impostazioni del programma(**Fig.3**).

Figura 3



Le schede a cui si può accedere sono:

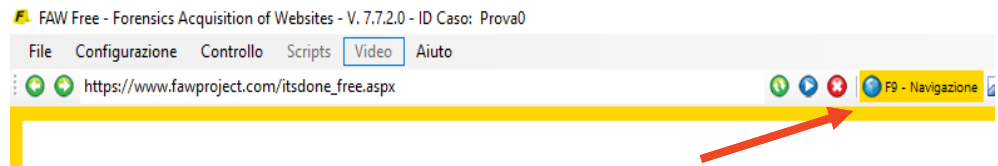
- **Generale:** impostazioni su lingua e server
- **Acquisizione:** scelta sulla destinazione del salvataggio dei file, è possibile attivare l'opzione di inserire data e ora dell'acquisizione anche sulla cornice (Gold box) che delimita l'area acquisita della pagina web
- **Oggetti collegati:** qua è possibile selezionare quali oggetti collegati alla pagina web salvare
- **Attività:** impostazioni sull'acquisizione video durante le attività svolte
- **File Host:** impostazioni sul salvataggio delle informazioni dettagliate sull'Host della pagina web



- *Acquisizione*: impostazioni sulla home page di default, sul caricamento di una copia certificante dei dati su server FAW, acquisizione traffico internet

### 3) Navigazione web

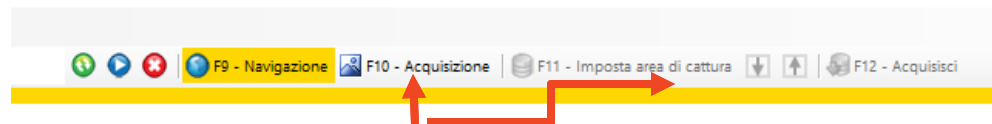
Figura 4



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(Fig.4).

### 4) Preparazione acquisizione

Figura 5



Cliccando su "Acquisizione" (Fig.5) FAW inizia ad acquisire, da quel momento, il traffico di rete e gli eventi del sistema operativo generati fino alla fine dell'acquisizione. In questa fase si può navigare fino alla pagina web desiderata; è consigliato fare partire questa registrazione prima di essere sulla pagina da acquisire per avere prova dell'accesso effettuato normalmente alla stessa (es. accesso con credenziali). Cliccando (o premendo il relativo tasto come tutti le altre fasi) su "Imposta area di cattura" è possibile cambiare a piacimento le dimensioni del *Gold Box* (rettangolo giallo) che racchiude l'area che viene catturata, il *Gold Box* può essere esteso verso il basso con la funzione di ridimensionamento o semplicemente trascinando il bordo con il puntatore del mouse. Bisogna precisare che, *il Gold Box* delimita l'area su cui verrà acquisita l'immagine ed alcuni oggetti collegati a quella porzione di pagina. Oggetti e dati generali, come per esempio il codice html, verranno acquisiti per tutta la web page indipendentemente dall'area delimitata dal Gold Box.

### 5) Acquisizione

Figura 6



Per iniziare l'acquisizione a questo punto è sufficiente cliccare su "Acquisisci" (Fig.6). FAW inizierà ad acquisire l'immagine della pagina Web facendola scorrere, poi

acquisirà gli headers e il codice HTML e gli eventuali oggetti contenuti nella pagina (se selezionati nel menu Configurazione).

Al termine delle operazioni si aprirà la finestra della cartella dove sono stati acquisiti i seguenti file (elenco dalla guida ufficiale FAW):

- **Acquisition.log**  
è il file che contiene l'elenco delle 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
- **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 HTM che contiene tutto il codice HTML della pagina web
- **CodeFrame{nomeframe}.htm**  
sono file che contengono il codice HTML del frame {nome frame} 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 adatte ad essere stampate a pagina intera su fogli A4
- **SystemLogEvents.txt**  
è il file in cui vengono registrati tutti gli eventi di Windows avvenuti durante l'acquisizione della pagina Web
- **screenCapture.wmv**  
è il file video acquisito da VLC con la cattura dell'intero schermo del computer dall'inizio dell'acquisizione fino alla fine

- **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**  
è la cartella che contiene tutti gli elementi della pagina Web acquisiti numerati progressivamente. Ogni acquisizione viene inserita in una sottocartella numerata sequenzialmente (esempio: 0001, 0002, 0003) della cartella con nome del Case ID scelta dall'utente.

#### 6) Verifica integrità acquisizione

Alla fine dell'acquisizione, è buona prassi verificare che i files dell'acquisizione non siano stati alterati; a tale scopo è presente la funzione "Controllo acquisizione": (Fig.7).

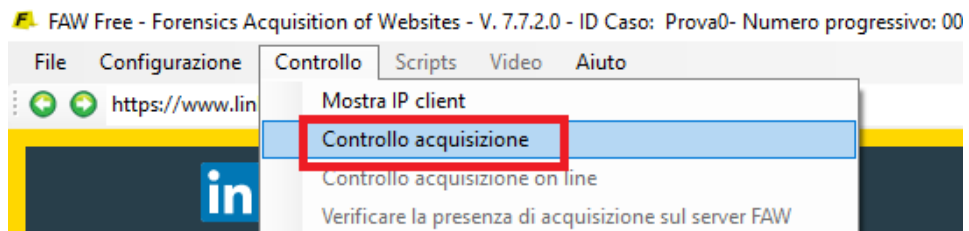


Figura 7

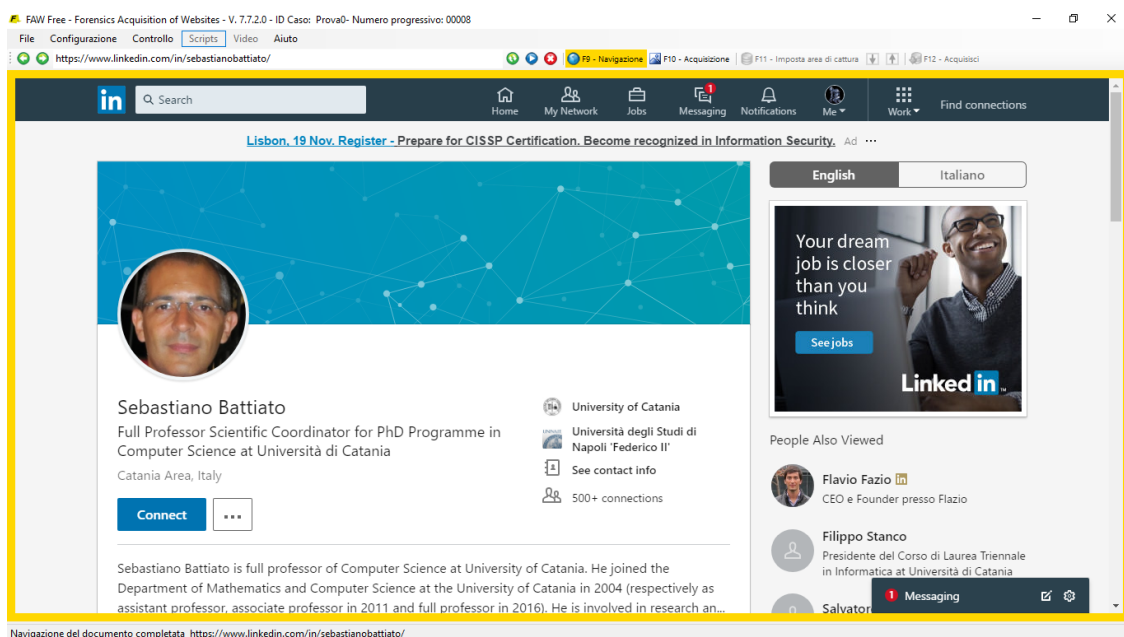
Una volta selezionata tale voce basterà selezionare la cartella dell'acquisizione da verificare. Se i dati dell'acquisizione sono stati salvati anche sul server FAW, è possibile eseguire una verifica dell'integrità dei files mediante confronto con i dati memorizzati nel database di FAW.

Se l'acquisizione venisse interrotta, forzatamente o no, si potrebbero trovare ugualmente i file salvati nella relativa cartella; in tal caso la verifica dell'integrità dell'acquisizione risulterebbe negativa.

## Esempio: acquisizione profilo LinkedIn

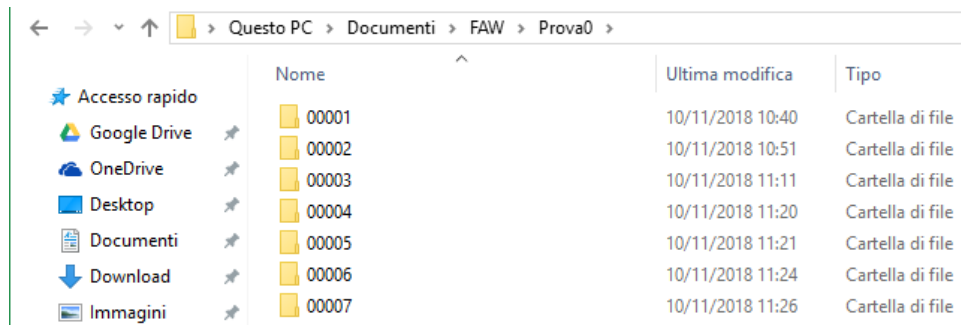
Passando ad un esempio pratico si vuole acquisire un profilo LinkedIn (home del profilo e ultimi post pubblicati). Viene usata la versione FAW free, che manca di molte opzioni fra cui il caricamento su server, la possibilità di produrre la registrazione video durante l'acquisizione ed il salvataggio di molti tipi di oggetti. Ciò comporterà la mancanza di alcuni dei file menzionati precedentemente e ci si concentrerà sui principali.

Figura 8



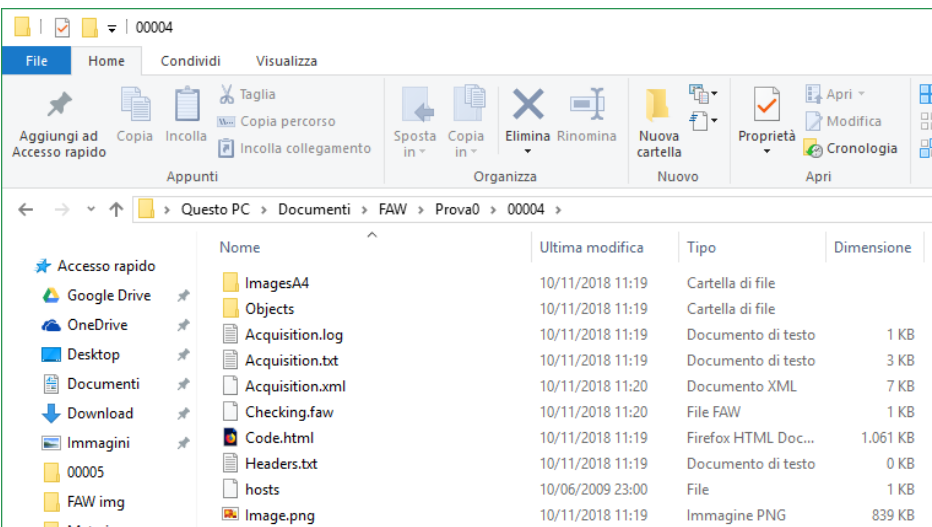
Dopo aver avviato la schermata iniziale chiamando il caso "Prova0", si è da subito attivata la registrazione delle informazioni a contorno dell'acquisizione, si è successivamente effettuato l'accesso al social e si è raggiunta la pagina web del profilo interessato(Fig.8). Seguendo a questo punto i passi rimanenti della procedura, già esposti nella sezione precedente, si sono svolte le acquisizioni della pagina principale del profilo e degli ultimi post. Infine si è svolto il controllo sulle diverse acquisizioni, ottenendo esito negativo in quelle interrotte e positivo in tutte le altre.

Figura 9



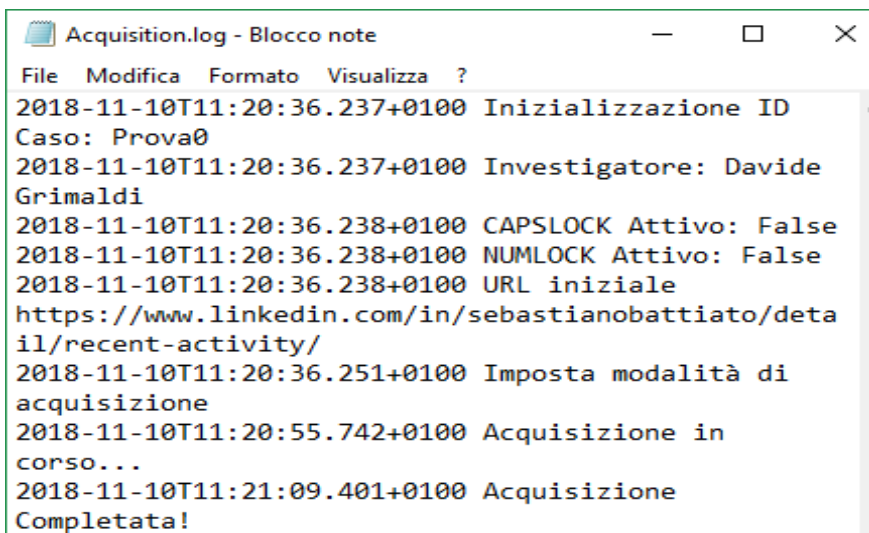
FAW ha creato automaticamente una sua cartella all'interno della directory "Documenti" e, al suo interno, quella del caso "Prova0" con le relative sottocartelle delle acquisizioni(Fig.9).

Figura 10



All'interno della cartella di un'acquisizione si possono vedere (Fig.10) i file che sono stati descritti nella sezione precedente. I più importanti sono: Acquisition.log; Acquisition.txt; Acquisition.xml; Checking.faw; essi sono infatti quelli da cui dipende l'integrità dell'acquisizione.

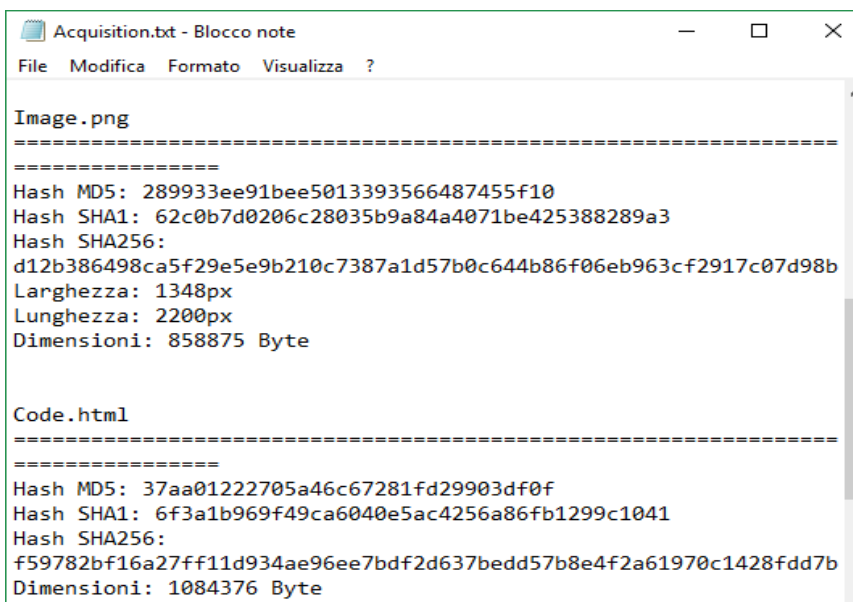
Figura 11



```
Acquisition.log - Blocco note
File Modifica Formato Visualizza ?
2018-11-10T11:20:36.237+0100 Inizializzazione ID
Caso: Prova0
2018-11-10T11:20:36.237+0100 Investigatore: Davide
Grimaldi
2018-11-10T11:20:36.238+0100 CAPSLOCK Attivo: False
2018-11-10T11:20:36.238+0100 NUMLOCK Attivo: False
2018-11-10T11:20:36.238+0100 URL iniziale
https://www.linkedin.com/in/sebastianobattiato/deta
il/recent-activity/
2018-11-10T11:20:36.251+0100 Imposta modalità di
acquisizione
2018-11-10T11:20:55.742+0100 Acquisizione in
corso...
2018-11-10T11:21:09.401+0100 Acquisizione
Completata!
```

L' Acquisition.log contiene oltre alle operazioni eseguite da FAW, con i relativi orari, anche alcune informazioni iniziali: ID del caso, investigatore, URL iniziale, stato di alcuni tasti della tastiera(Fig.11).

Figura 12



```
Acquisition.txt - Blocco note
File Modifica Formato Visualizza ?

Image.png
=====
Hash MD5: 289933ee91bee5013393566487455f10
Hash SHA1: 62c0b7d0206c28035b9a84a4071be425388289a3
Hash SHA256:
d12b386498ca5f29e5e9b210c7387a1d57b0c644b86f06eb963cf2917c07d98b
Larghezza: 1348px
Lunghezza: 2200px
Dimensioni: 858875 Byte

Code.html
=====
Hash MD5: 37aa01222705a46c67281fd29903df0f
Hash SHA1: 6f3a1b969f49ca6040e5ac4256a86fb1299c1041
Hash SHA256:
f59782bf16a27ff11d934ae96ee7bdf2d637bedd57b8e4f2a61970c1428fdd7b
Dimensioni: 1084376 Byte
```

Acquisition.txt contiene anche un elenco di tutti i file dell'acquisizione con i relativi codici Hash (l'equivalente delle impronte digitali per un oggetto informatico) e le dimensioni(Fig.12).

### Extra: ID LinkedIn

Per identificare in modo certo un profilo sui social network non è sufficiente il nome del profilo o l'URL della pagina, bisogna risalire al suo ID univoco che permette di ritrovare il medesimo anche in caso di modifiche al nome.

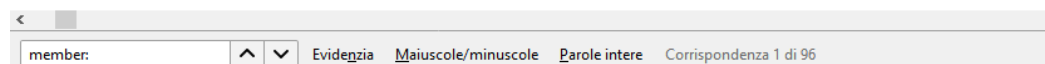
Per LinkedIn la procedura per ottenere l'ID di un profilo è la seguente:

- 1) Accedere al profilo interessato
- 2) Visualizzare il codice sorgente della pagina: ogni browser permette questa funzionalità, di solito con una voce nelle opzioni del tipo "Visualizza sorgente pagina"
- 3) Cercare all'interno del sorgente, con uno strumento di ricerca testo, la parola chiave "member:"
- 4) Copiare o annotare il numero che segue (**Fig.13**)

Al fine della raccolta delle prove in caso di diffamazione è molto più efficace partire dal codice ID del profilo.

Figura 13

```
ot;segmentIndex";:1,&quot;treatmentIndex";:0,&quot;urn";:&quot;urn:li:member:358479358";
```



### Trattamento dati acquisiti

Come per tutti i reperti informatici valgono le *best practices* del settore; oltre queste, per validare i dati acquisiti, è necessario firmare digitalmente il file "Acquisition.txt" o "Acquisition.xml" ed apporvi una *marca temporale*. Quest'ultima ha la funzione di certificare data ed ora dell'acquisizione.

"La **Marca Temporale** è un servizio che permette di **associare data e ora certe e legalmente valide ad un documento informatico**, consentendo quindi di associare una validazione temporale opponibile a terzi." (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005).

Le marche temporali possono essere acquistate online da un fornitore di servizi informatici, devono essere conformi al regolamento eIDAS (Regolamento UE n° 910/2014 sull'identità digitale.) ed hanno validità a livello europeo. Per l'utilizzo del servizio di *Marcatura Temporale*, è necessario acquistarle ed essere in possesso di apposito software, di solito fornito dal venditore.

## Riferimenti

---

- 1.1 Reato di diffamazione:  
<https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-ii/art595.html>
- 1.2 Articolo La Stampa Umberto Eco  
<https://www.lastampa.it/2015/06/10/cultura/eco-con-i-parola-a-legioni-di-imbecilli-XJrvezBN4XOoyo0h98EfiJ/pagina.html>
- 1.3 Documentazione FAW  
<https://it.fawproject.com/la-storia-di-faw/>  
<https://it.fawproject.com/guida-6-1/>
- 1.4 Marca temporale  
<https://www.pec.it/marche-temporali.aspx>