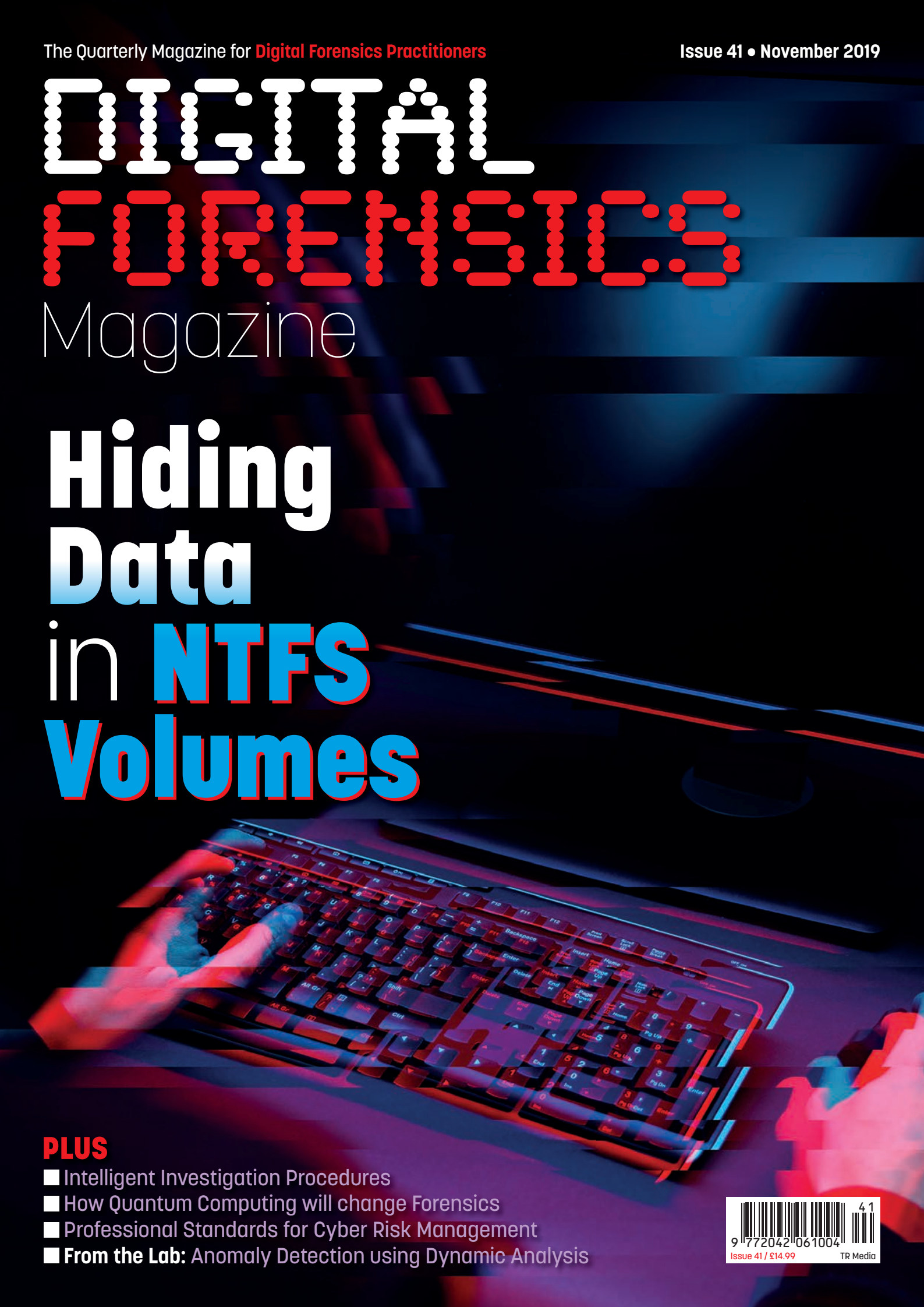
The Quarterly Magazine for Digital Forensics Practitioners

Issue 41 • November 2019

DIGITAL FORENSICS Magazine

Hiding Data in NTFS Volumes



PLUS

- Intelligent Investigation Procedures
- How Quantum Computing will change Forensics
- Professional Standards for Cyber Risk Management
- **From the Lab:** Anomaly Detection using Dynamic Analysis

41
9 772042 061004
Issue 41 / £14.99
TR Media

FAW

Forensics Acquisition of Websites

The first forensic browser that can easily, quickly
and legally acquire any type of web page.

FAW manages the acquisition flow of web pages in a totally automatic way avoiding therefore the risk of human error of manual procedures.

FAW can be used by lawyers, notaries, private citizens, companies, organizations and associations in a simple and intuitive way without having technical computer skills; but also from technical consultants, digital forensics experts, investigators and law enforcement agencies who are looking for a product with advanced features capable of speeding up acquisition operations, thus optimizing time and resources.

PRODUCT UPDATE

Welcome to the new Product Update section of the magazine. Over the last few years of publishing *Digital Forensics Magazine* we have noticed a significant rise in the development of tools to automate the process of carrying out a digital investigation.

As a magazine we are constantly receiving news of updates to established products or of new products that are being released. Our plan is, therefore, to bring you a selection of these new products and product updates that we have received during the previous quarter.

Of course, we will not be able to include all that we receive so we will be making some editorial decisions along the way, however, those updates we select will be considered by the editorial team as the most significant and noteworthy to our discerning *DFM* readers.

To get us started we asked the FAW Project to provide a detailed explanation of their new release of FAW 8, that has been updated to include the capability to investigate Facebook accounts.

If you are a vendor and believe that you have a product release or new product that hould be included, do get in touch.

Forensics Acquisition of Websites (FAW) software, was created as a browser utility for the acquisition of web pages with Legal Value. FAW was developed in compliance with national and international regulations and the best practices of Digital Forensics.

For the acquisition of web pages to be considered valid and effective as evidence in a judicial procedure it is necessary to comply with strict procedural legal rules as well as to follow best practices recognized by the forensic scientific community and experts in the field of digital forensics. FAW is an innovative software application that combines the strictness of the acquisition method with the simplicity of use.

The value of the digital proof is based on the methods with which it is acquired. In order for a digital datum to become proof, it is necessary to guarantee certainty and conformity between the forensic acquisition carried out and the web page present on the Internet. Utilising advanced automation and security features, the possibility of counterfeiting or operator errors is absent, so FAW complies with the ISO/IEC 27037 directives and can be immediately presented at trial or extra judicial proceedings.

FAW is a suite of forensic tools useful for acquisition of all type of web sites and other resources providing the following functionality:

- **FAW TOR**, is for web page acquisition of the 'Darkweb' within the TOR network;
- **FAW STOP** allows the manual starting and stopping of web page acquisition, it allows the operator to capture the behaviour of pages and multimedia content (audio/video);
- **FAW TIME** allows you to capture content at different times of the day;
- **FAW BOT** is a web crawler that searches all the web pages that relate to the main page, extracting the URL and headers to create an index from where you are able to do successive automatic acquisitions. It also allows research within web sites with login to protected areas, for example social networks;
- **FAW MULTI** is the multi-page FAW version and it allows the automatic capture of a list of web pages. It is suitable for fast and automatic capture of complete web sites;
- **FAW FTP** You are able to capture full websites with FTP mode without any edit to the copied files metadata.
- **FAW REPORT** allows the creation a detailed report of all activities within the FAW suite, utilising a full custom template.
- **FAW FACEBOOK** is the latest module for the automatic acquisition of Facebook content.

The software suite specifically allows for the:

- Acquisition of the entire HTML code of the web pages including saving the headers;
- Acquisition of all the objects connected to the web page (images, archives, documents, executables and scripts) whose control hashes will be inserted in the Acquisition.xml file;
- The acquisition of different types of images and analysis of all pages containing data streaming (e.g. video);
- The ability to make a partial acquisition of the web page, based on the investigator's needs, by choosing a specific area of interest. ▷

Figure 1. The Facebook Menu Selection

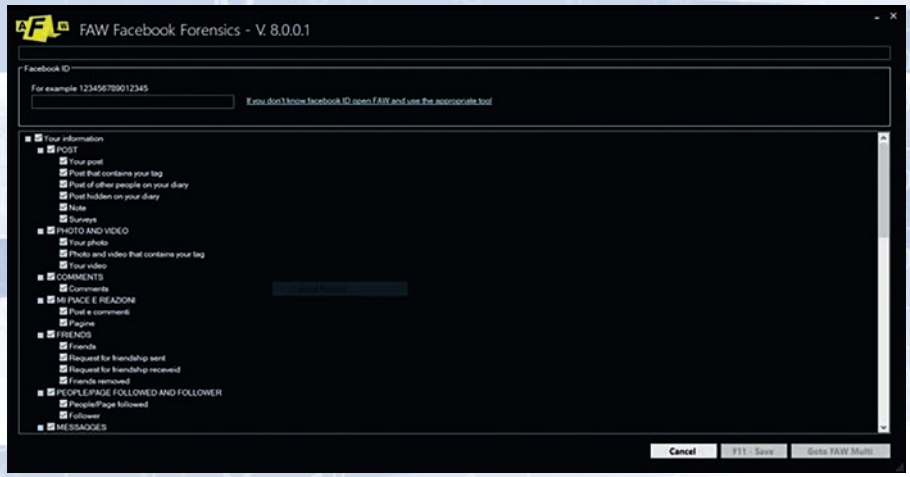


Figure 2. The Facebook Acquisition Menu

FAW allows for the acquisition of pages accessible only through the HTTPS protocol (e.g. Facebook pages), obviously already having the credentials to access the resource (username and password); this allows the digital forensics practitioner to also acquire the content of any chat made via Facebook. The software is presented as a browser (Chromium Web Browser) through which it is possible to access the web resource, starting with the acquisition of the HTML code of the page, its headers and all the objects within the content.

It is also possible to obtain video recording (ScreenCapture.mp4) of the acquisition operation and network traffic dump (file.pcap) related to the operations performed, thanks to the FAW interaction with the WireShark application (www.wireshark.org) and VLC (www.videolan.org).

The function of making it possible to record the forensic operation as it is carried out, is something that non digital forensics experts (e.g. Judges, Lawyers, etc.) like and by having all of the technical data from the acquisition along with results of the test (hash, logs, etc.), even after many years, there is the possibility of reviewing all the steps of the technical investigation as it was carried out. Once the acquisition process has been completed, FAW generates several files, stored in a folder named with the 'CaseID' chosen by the investigator at the time the application is run. The application generates an 'Objects' folder containing:

- All the elements of the Web page acquired numbered progressively,
- Image files (screenshots) of the acquired resource,
- .wmv file (video recording of operations),
- file.pcap (network traffic dump),
- All the html code of the web page (code.html),
- Headers sent to the browser from the web page (headers.txt),
- The Acquisition.log log file
- Checking.faw (the file contains a control code that allows you to check whether the Acquisition.txt and Acquisition.xml files have been altered over time);
- Acquisition.txt and Acquisition.xml (files in different formats containing all the references of the acquisition carried out with relative MD5 and SHA1 hashes).

The files mentioned above are the most important as it is these that demonstrate the non-alteration of the files produced during the investigation. FAW allows using the "Acquisition checking" function available in the "Checking" menu to verify the integrity of the two files Acquisition.txt and Acquisition.xml.

The application of the software is purely forensic, the software calculates the MD5, SHA1 and SHA256 hashes of all the acquired files, producing a detailed log of the operations carried out with relative references (Acquisition.log). The application is able to certify the location where the acquisition was carried out, through the relative IP and identification of the station, also offering the possibility of adding additional time verification (date and time of the acquisition operations), the acquisition is made to a certified PEC e-mail box.

Furthermore, through the application it is possible to acquire and "capture" a chat conversation, for example via Facebook. Having access credentials, and consequently accessing a web page accessible exclusively via the HTTPS protocol. With this application it is also possible to make forensic copies also of portals that offer the certified electronic mail service. FAW is a complete software package that allows you to comply with all the best practices of forensic computing for the acquisition of web content.

The New FAW Module for Acquiring Facebook Pages

The acquisition of Facebook pages is one of the most common requests made of digital forensic investigators and law enforcement agencies that use FAW to extract digital evidence. With version 8 of FAW, a module has been added dedicated to optimizing and speeding up the acquisition of complete Facebook profiles and the acquisition of comments on Facebook pages. The new module is accessed from the initial FAW window by clicking on the easily recognizable button called Facebook (Figure 1)

The window that opens (Figure 2) allows you to enter the Facebook user ID and choose which Facebook profile pages to acquire automatically.

FAW allows for the acquisition of pages accessible only through the HTTPS protocol.

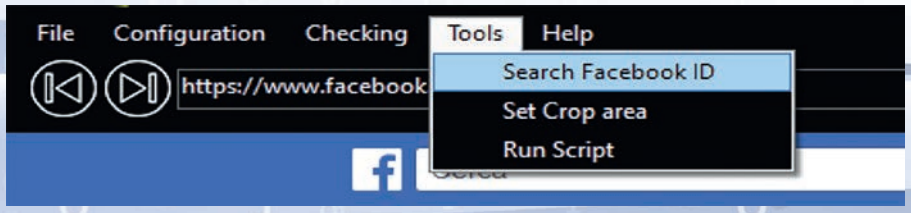


Figure 3. The Search for Facebook ID Function

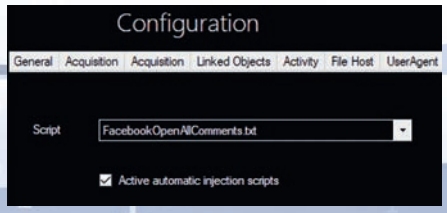


Figure 4. Script Injection

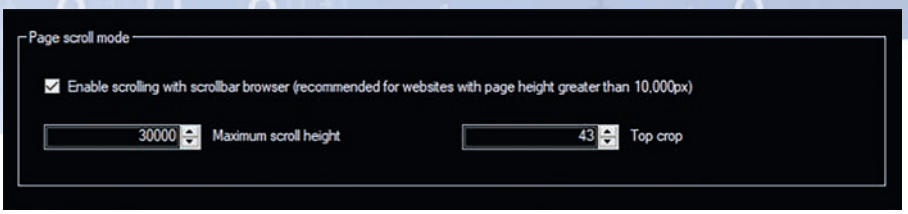


Figure 5. Script Function

If you do not know the Facebook ID, you may use the tool integrated in FAW to retrieve it from a profile page. To use this tool, simply open FAW, log into Facebook by logging in with your credentials and reach the profile page of the person whose Facebook ID you want to recover. Then open the "Tool" menu and click on "Search Facebook ID" (Figure 3).

The Facebook ID will be retrieved and automatically switched to the Facebook module of FAW (Figure 2). From this module it is possible to acquire all the information, public and private, of the user profile as long as you are logged in with the credentials of the profile that is the object of acquisition, or all public information if one is logged in with a different user. The pages that can be acquired are the following:

- POST: Your posts, Posts containing your tag, Posts of other people in your diary, Posts hidden by your diary, Nets, Polls.
- PHOTOS AND VIDEOS: Your photos, photos and videos containing your tag, your videos.
- COMMENTS: Comments.
- I LIKE AND REACTIONS: Post and comments, Pages.
- FRIENDS: Friends, Friend requests sent, Friendship requests received, Friends removed.
- PEOPLE / FOLLOWING PAGES
- ND FOLLOWER: People / Pages followed, Followers.
- MESSAGES: Your messages.
- GROUPS: Your groups, the activities of group members, your posts and comments in groups.
- EVENTS: Your events, Your event responses, Event invitations.
- PROFILE INFORMATION: Your contact information, Information about you, Important events, Your music.
- PAGES: Your pages.
- MARKETPLACE: Items sold.
- PAYMENT HISTORY: Payment history.
- SAVED ELEMENTS AND COLLECTIONS: The items you saved, Collected.
- YOUR PLACES: Places you have created.
- APP AND WEBSITES: Apps and websites, Your apps, App posts and websites.
- OTHER ACTIVITIES: Poke, interactive videos.
- INSERTIONS: Advertising interests, Advertisers who have uploaded a list of contacts containing information about you, Advertisers with whom you have interacted.
- INFORMATION ABOUT YOU: Facial recognition, your address book, videos you have watched.
- SEARCH HISTORY: Your search history, Videos you've searched for.
- POSITION: Chronology of positions, main location.
- INFORMATION ON PROTECTION AND ACCESS: Where you have logged in, Authorized accesses.

Once the Facebook ID has been entered and the items to be acquired have been selected, press the [Save] button to save an XML file containing all the URLs of the pages to be acquired complete with the Facebook ID; or you may automatically switch to the FAW MULTI tool and start the acquisition of all pages.

Facebook Page Acquisition with Automatic Opening of All Comments

For the opening and acquisition of comments to Facebook posts automatically, the option of automatic Script injection has been provided in the "Script" section (Figure 4).

For this type of acquisition, it is advisable to use the "Page scroll mode" (Figure 5) setting a maximum height sufficient to contain the entire page with all comments open.

After enabling the requests and settings, simply navigate to the Facebook page with the comments you want to capture and start a normal acquisition. FAW will initially scroll the page to receive all the data from the server, then it will reposition itself at the beginning, inject the script and perform the acquisition of the entire page.

Summary

FAW is the only digital forensics browser in the world that guarantees the authenticity, conformity and inalterability of the acquired web pages. The continuous innovations introduced and designed to automate and speed up the acquisition of Web pages make FAW the reference software used by consultants and law enforcement agencies around the world. FAW, as always, is the only innovative forensic browser. FAW is a software application downloadable from **www.fawproject.com**.