SUBROSASOFT's

MacForensicsLab Web Agent

Copyright © 2010

Trademarks

Credits:

With thanks to the following people for their involvement in the creation of this manual: Ben Brausen.

Typeface:

Officina Sans Book is the typeface used in all sections and text portions of the document.

Table of Contents

Overview of MacForensicsLab Web Agent

This section provides an overview of MacForensicsLab Web Agent and it's features, functionality and design.

About MacForensicsLab Web Agent

Welcome to MacForensicsLab Web Agent. If this is your first time using SubRosaSoft.com Inc.'s software, be assured you made the right decision. SubRosaSoft.com Incorporated is the world-wide leader in Macintosh-based forensics, with many federal, state and local law enforcement organizations around the globe using our software. In addition, our lines of forensic software is used by the military, intelligence community, and many privately owned and operated organizations seeking a powerful and innovative forensic solution.

As a company, SubRosaSoft.com Incorporated is dedicated to providing forensic solutions that not only meet and exceed your expectations but that change the way modern computer forensics are performed. Traditional computer forensic software development has mirrored the needs of traditional law enforcement by developing a solution only as a problem presented itself. In doing so, law enforcement is left without a timely answer to their technological dilemma. When the momentum of an investigation suffers due to a purely reactive development cycle, criminals go unpunished and victims are left needing resolution or worse, new victims are created. SubRosaSoft.com Inc. seeks to change that paradigm by offering expandable and scalable solutions that can adapt to an organization's needs and anticipate problems through use of intelligent proactive development.

SubRosaSoft.com Inc. understands how difficult it has become to keep pace with technology. All too often, forensic examiners are understaffed and overworked, making the environment ripe for case backlogs and an increasing potential for errors. In an effort to minimize these conditions, SubRosaSoft.com Inc. leverages technology and its advancements to allow for fewer mistakes. By doing so, our forensic solutions aid in maximizing the efficiency and effectiveness of its users, thereby getting more done with less mistakes.

SubRosaSoft.com Inc. is dedicated to our mission of providing powerful, easy-to-use, cost-effective forensic solutions that help you achieve your organization's forensic goals. To this end, we offer products that cover the entire spectrum of computer forensics, not just the static lab-based solution. Modern technologies demand integration throughout the forensic process and SubRosaSoft.com Inc. accounts for this evolution with solutions for incident response, triage, static examinations and reporting. In summary, SubRosaSoft.com Inc. views mission accomplishment as a corporate social responsibility, one we take very seriously and as such we strive to become not only a software development company but a partner to all our customers.

MacForensicsLab Web Agent allows forensics examiners and detectives to crawl websites in search of illicit images. With a built-in skin tone analyzer, Web Agent narrows down the search for images of interest. Reporting is a breeze with the customizable HTML format. URLs and hash numbers of the images are generated to ensure the accuracies of the report.

MacForensicsLab Web Agent is cross-platform, allowing users to run it natively on Windows XP, Windows Vista, Windows 7, and Linux (RedHat, Ubuntu and SuSe).

System Requirements

Overview

This section covers the basic and recommended system requirements for successfully running MacForensicsLab Web Agent. Modern forensic processes require not only powerful systems to process the massive amount of data, but a scalable solution designed to harness the system resources for greater speed and increased functionality. Nevertheless, MacForensicsLab Web Agent has been specifically optimized for efficiency and speed through the use of appropriate memory allocation and a multi-threaded design.

Mac OS X Requirements

-Apple Macintosh G4 800MHZ or faster (Intel based Mac recommended)

-Mac OS X (version 10.4 or newer)
-1 GB of RAM
-Internet Access

Windows Requirements

-Processor 800MHZ or faster
-Windows XP/Vista/7
-512 MB of RAM
-Internet access

Linux Requirements

-Processor 800MHZ or faster
-x86-based Linux distribution with GTK+ 2.0 (or higher), glibc-2.3 (or higher) and CUPS (Common UNIX Printing System)
-512 MB of RAM
-Internet Access

We officially support the following:
-SUSE Linux Enterprise Desktop
-Red Hat Enterprise Linux Desktop

Registration Number

Each user is required to have a registration number, otherwise known as a serial number, in order to complete the full version installation of the software properly. Whether the software has been purchased online or through a third party retail channel, the user needs the registration number when preparing for installation of the software.

Online Purchase

When purchasing the software online at: http://www.MacForensicsLab.com/, the registration number is automatically emailed as part of the purchase confirmation. If a confirmation email is not received, please ensure that it has not mistakenly been placed in the email client's junk folder before requesting technical support. Having received

the email, please make a print out and store this in a safe and secure place for future reference.
Note: A serial number is not required for the special Flash Key based version.

Retail Purchase

If the software was purchased through a retail channel, the registration number should be inside the DVD case. Please be sure to keep these details in a safe and secure place.

Updates and Upgrades

A single registration number is valid for incremental updates to the purchased version of MacForensicsLab Web Agent. When upgrading between versions the purchase of a new registration number will be required. For information on upgrades, please email sales@subrosasoft.com.

Lost Registration Number

Please ensure that you keep your registration number in a safe and secure place. Print off confirmation emails or back them up. SubRosaSoft Inc. cannot guarantee the ability to re-issue serial numbers for our users.

Site Licenses

Site Licences can be purchased online via http://www.subrosasoft.com/. For volume discounts please contact us directly via email: sales@subrosasoft.com.

Downloading from the Web Site

It is important for any user to ensure that they have the latest version of the MacForensicsLab Web Agent software. The latest version is always freely available for download on our web site at: http://www.MacForensicsLab.com/

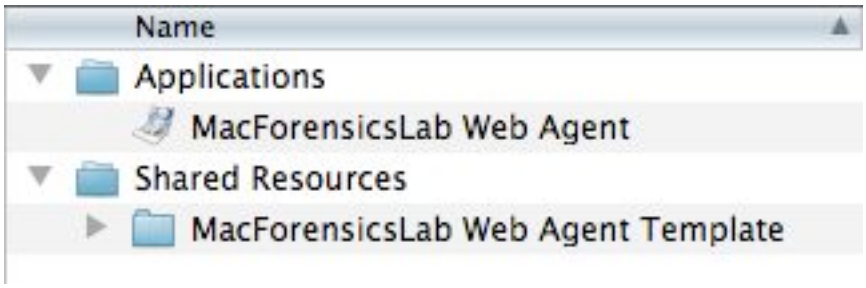
A download link, alongside version information, is accessible on the product page of the site. Simply click the respective link and a compressed archive file will automatically begin to download to the desktop, or another specified download location.

MacForensicsLab Web Agent versions are distributed in a ZIP archive format and can be decompressed in the Mac OS X Finder with a simple double-click of file icon. This will

place the decompressed application file in the same location as the original ZIP archive, most likely the Downloads folder. With Windows and Linux based systems. you may need to download a third party utility to decompress the zip file.
Note: The software can be run directly from the special Flash Key based version.

Installation From the Disk Image

Having decompressed the folder, copy both the 'Applications' and the 'Shared Resources' folder from the MacForensicsLab Web Agent folder to your computers 'Applications' or the 'Desktop' folder. Note that the folder structure with the 'Shared Resources' folder being located one directory down from the MacForensicsLab Web Agent application must be maintained although the name of the folder containing the application can be changed. Some users may choose to create a MacForensicsLab Web Agent folder and then store the folder containing the application and the 'Shared Resources' folder within that.



Installing From the CD-ROM

Once the CD-ROM has mounted on the user's desktop and the CD-ROM volume has been opened into a window, the user should see a folder named "Applications". To install MacForensicsLab Web Agent to the host computer, drag & drop MacForensicsLab Web Agent folder to any desired location on the new host computer, though we strongly recommend placing it in the host computer's "Applications" folder. Having done this the user is ready for the initial setup.

Uninstalling MacForensicsLab Web Agent

MacForensicsLab Web Agent is a completely self-contained application and requires no special functionality to uninstall it. The procedure to uninstall MacForensicsLab Web Agent is to navigate to the directory in which the MacForensicsLab Web Agent folder is

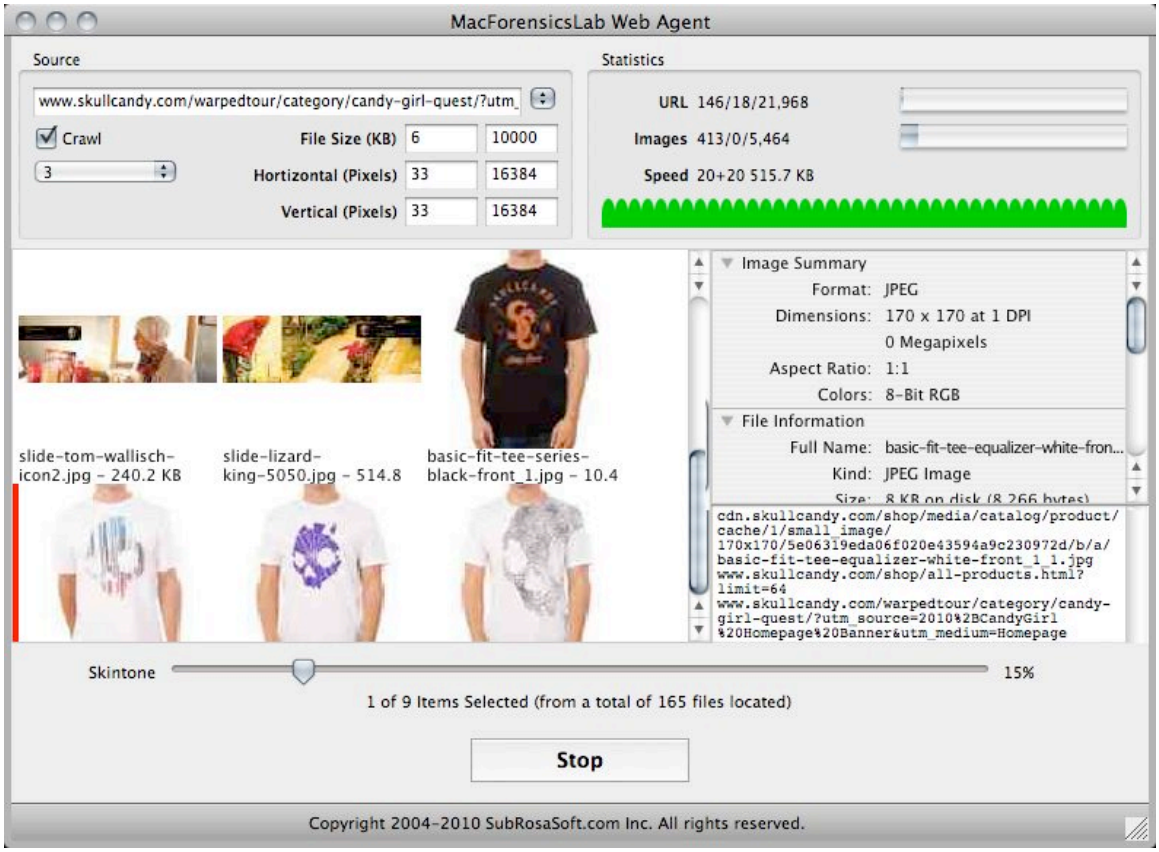
currently installed, highlight the MacForensicsLab Agent folder and either drag and drop it into the Trash or delete it using the delete key.

Initial Setup

The first time the application is launched the user will be asked accept the End User License Agreement (EULA – see Appendix C) and then to enter a valid registration number. After the registration number has been entered, the user will then be taken to the 'Main Window'.

Elements of MacForensicsLab Web Agent

Designed for non-technical personnel, Web Agent is extremely easy to use; there is no rebooting, troubleshooting or complex interfaces. It can run natively on Mac OS X, Microsoft Windows, and Linux to search illicit sites. By quickly providing images relevant to an investigator's interests, MacForensicsLab Web Agent is an invaluable tool to all law enforcement agencies. Web Agent has the ability to save files of interest or generate an HTML report with thumbnails, locations of files, site addresses, hash information, dates, and related server information of any or all files.



The 'Source' area

The source window is where the user sets the criteria for the search.

The first required field is the URL for the site and directory the investigator would like to examine. This URL is entered without the HTTP prefix. To the right of the URL field

is a drop-down menu that allows the user to select previously entered websites. To clear the sites listed, simply select '**Clear**' from the bottom of the drop-down menu.

Below the URL field is a checkbox marked '**Crawl**'. With this box checked, MacForensicsLab Web Agent will search links on the depth indicated in the drop-down menu below the '**Crawl**' checkbox.

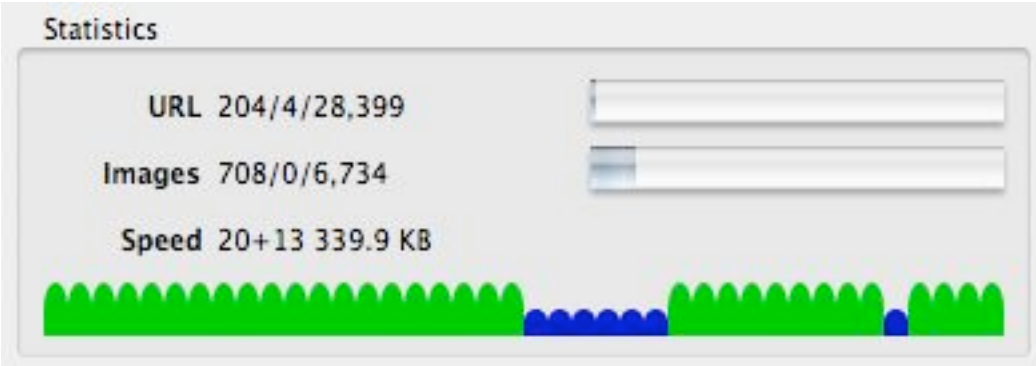
'**File Size (KB)**' allows the user to set requirements for images displayed based on the file size measured in kilobytes. The first box sets the minimum size requirement and the second box sets the maximum size requirement.

'**Horizontal (Pixels)**' allows the user to set the requirements for images displayed based on the number of horizontal pixels in the image. The first box sets the minimum size requirement and the second box sets the maximum size requirement.

'**Vertical (Pixels)**' allows the user to set the requirements for images displayed based on the number of vertical pixels in the image. The first box sets the minimum size requirement and the second box sets the maximum size requirement.

The 'Statistics' area

While a search is running, statistical information about the process is displayed in the 'Statistics' area in real-time.



'**URL**' displays 3 sets of separated numbers. Starting from the far right, the first number is the number of pages discovered to download. The middle number shows the number

of pages downloaded but still waiting to be processed/parsed. The number on the left shows the number of URLs downloaded and processed so far.

'**Images**' displays 3 sets of separated numbers. Starting from the far right, the first number is the number of images discovered to download. The middle number shows the number of images downloaded but still waiting to be processed/parsed. The number on the left shows the number of images downloaded and processed so far.

'**Speed**' displays two numbers as '**xx + xx**'. The first number is the number of the total 40 sockets (connections) that are downloading webpages. The second number is the number of sockets downloading images. The current download speed of those connections is displayed next to these two number sets.

The 40 humps or bubbles below the '**Speed**' display shows the state of the 40 socket connections. Blue indicates the connection is idle and green indicates the connection is in use.

The thumbnail area

As a search runs, images that meet the criteria set forth in the '**Source**' area are displayed in the thumbnail area of the Web Agent window. Clicking on any of these images will display information about the file in the '**File Information**' area.

The Skintone slider below the thumbnails can be used to show or hide images based on percentage of skintones within the image. By default this slider is set to 15% as that has been found to be the optimal range to eliminate many non-human pictures without hiding too many false positives. Increasing this slider will increase the percentage of skintone that must be present in the image to be displayed in the thumbnail area. Decreasing the slider to 0% will display all images in the thumbnail area.

The 'File Information' area

Information about images that are selected in the thumbnail area is displayed in the 'File Information' area. This contains information like format, dimensions, aspect ratio, colors, file name, size and more. Much of the information displayed in the 'File Information' area is dependent on the metadata contained within the image file itself.

Running MacForensicsLab Web Agent

Configuring MacForensicsLab Web Agent

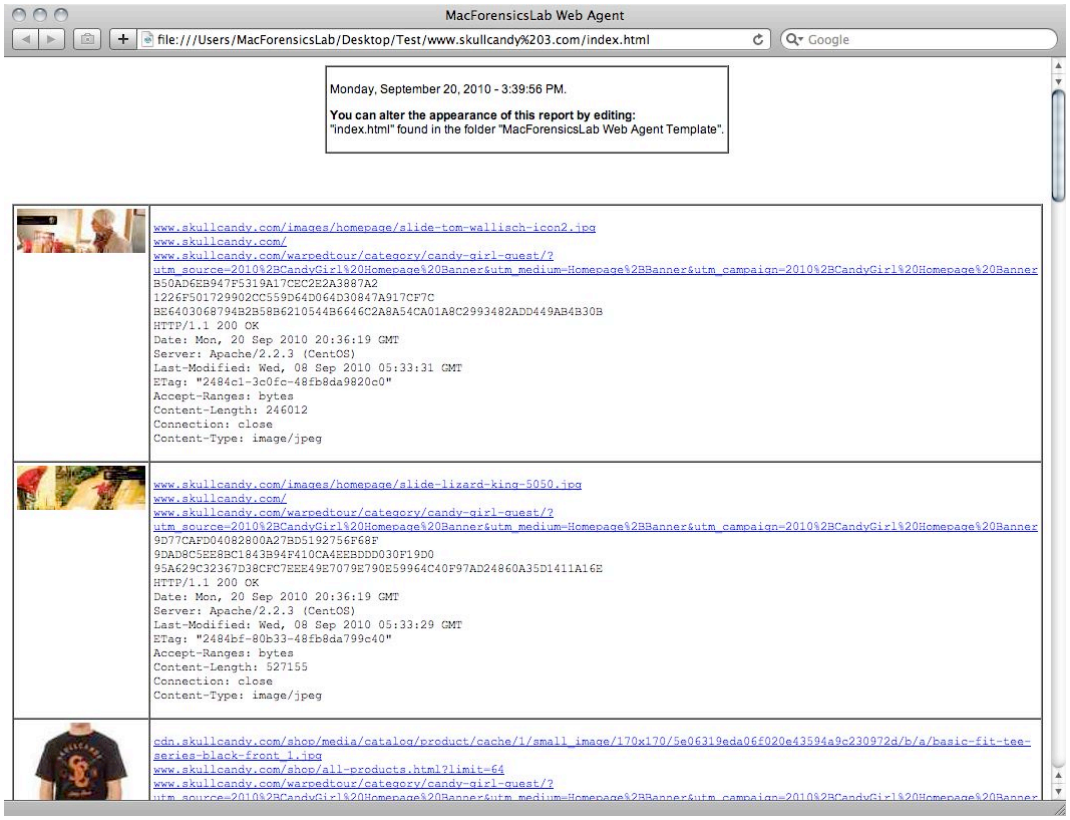
The first step in configuring Web Agent is entering the URL the user desires to examine. Once they have entered the URL, the user should then set the options including File Size, Horizontal and Vertical pixels. They must also select if they would like the URL to be crawled and if so, to what depth using the drop-down menu. Once these options have been set, the user can click the **Start** button at the bottom of the window. The user will then be prompted to select a folder to save the downloaded data to. Once a folder has been selected, the search will begin. Once the search has started, statistics will be displayed in the '**Statistics**' area and images will start to appear in the thumbnail area. Clicking on images in the thumbnail area will display more information about them in the '**File Information**' area.

Saving images

Users may select one or more images to be saved to the location of their choice. To do this, click on the image (or Command-Click on a Mac and Option-Click on a PC to select multiple images) the user wishes to save. Then select **Save** from the **File** menu. The user will be prompted to select a location to save these images. Select the location and click the Save button. The images will be saved in the desired location in a folder labeled with the website's name.

Writing a report

To write a report, first select the images to include in the report. Once the images are selected, choose **Write Report...** from the **File** menu. The user will be prompted to select a location to save the report. This is the location the report will be written to in a folder labeled with the website address along with a folder containing thumbnails and the actual images. Once the location has been selected, click the **Choose** button. A progress window will be displayed briefly while the report is written.



Once the report has been written, it will automatically be opened in the default web browser. The report will show the selected images along with where the image was found with a link to both the HTML page and the URL of the actual image, information about each image plus hash numbers in three different standards (MD-5, SHA-1, and SHA-256).

The report formatting can be change by editing the HTML file titled **index.html** containing in the **MacForensicsLab Web Agent Template** folder within the **Shared Resources** folder in the same directory as the MacForensicsLab Web Agent application.

Getting Help and Technical Support

Finding Help within MacForensicsLab Web Agent

Help can be found both via the small, context sensitive information clips that appear when the examiner rolls the mouse over a window element, as well as the standard help menu at the top of the screen. Contextual tool tips include buttons and parts of MacForensicsLab Web Agent that require some form of user interaction.

On the Web

We provide over 100 links to forensic resources, manuals, a complete knowledge base and a plethora of additional information on our website. For updates, resources and additional information please visit:
http://www.MacForensicsLab.com

Technical Support

We provide free technical support both via email or phone during the hours **10am** to **6pm** Pacific Standard Time (GMT -8) **Monday** to **Friday**. By email, we can be reached at the following address: support@macforensicslab.com. By phone, we can be reached at: +1 (510) 870 7883, or by fax on +1 (510) 868 3407.

In addition to any support question(s), the examiner must include **ALL** of the following pieces of information:

-Valid registration number or purchase information.
-System configuration(s) – hard drive make, model etc.
-System OS version.
-System related information can be found by using the “System Profiler” application in the -/Applications/Utilities folder.

Comments and Questions

If you have comments, problems, or questions about this product, or if you are interested in a site license, please contact us via email: info@macforensicslab.com

Company Address

SubRosaSoft.com Inc.
5387 Diana Common
Fremont, California 94555
http://www.SubRosaSoft.com

End User's License Agreement (EULA)

End Users License Agreement

SubRosaSoft.com Incorporated's End Users License Agreement

EULA

DO NOT USE THIS SOFTWARE UNTIL YOU HAVE CAREFULLY READ THIS AGREEMENT AND AGREE TO THE TERMS OF THIS LICENSE. BY USING THE ENCLOSED SOFTWARE, YOU ARE AGREEING TO THE TERMS OF THIS LICENSE.

The software license agreement for this program is included in this manual so you can read it before installing the program. INSTALLING THE PROGRAM OR USE OF THE MATERIALS ENCLOSED WILL CONSTITUTE YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT. If you do not agree to the terms of this software license agreement, do not install the software and promptly return the package to the place of purchase for a full refund of all money that you paid for the product.

In return for purchasing a license to use the computer program known as "MacForensicsLab™" and for purchasing documentation included in this package, you agree to the following terms and conditions:

1. License. The software enclosed is licensed, not sold, to you by SubRosaSoft.com Inc. for use under the terms of this software license. This non-exclusive license allows you to:

i. Use MacForensicsLab Web Agent™ software only on a SINGLE computer at any one time. You may only use the MacForensicsLab Web Agent software and only on drives physically connected to that single CPU.

ii. Only use the software to monitor systems on a SINGLE computer that is used by you.

iii. Make one copy of software in machine-readable form, provided that such copy is used only for backup purposes and the copyright notice is reproduced on the backup copy.

iv. Transfer software and all rights under this license to another party together with a copy of this license and all documentation accompanying the software, provided the other party agrees to accept the terms and conditions of this license.

As a licensee, you own the media on which the software is originally recorded. The software is copyrighted by SubRosaSoft.com Inc. and proprietary to SubRosaSoft.com Inc., and SubRosaSoft.com Inc. retains title and ownership of the software and all copies of the Software. This license is not a sale of software or any copy. You agree to hold software in confidence and to take all reasonable steps to prevent disclosure.

2. Restrictions. You may NOT distribute copies of this software to others or electronically transfer software from one computer to another over a network or via modem. The

software contains trade secrets that are wholly owned by SubRosaSoft.com Inc. You may NOT decompile, reverse engineer, translate, disassemble or otherwise reduce the software to a human understandable format. YOU MAY NOT MODIFY, ADAPT, TRANSLATE, RENT, LEASE, RESELL FOR PROFIT, DISTRIBUTE, NETWORK, OR CREATE DERIVATIVE WORKS BASED UPON THIS SOFTWARE OR ANY PART THEREOF.

3. Termination. This license is effective until terminated. This license will terminate immediately without any notice from SubRosaSoft.com Inc. if you fail to comply with any of its provisions. Upon termination you must destroy the software and all copies thereof. You may terminate this license at any time by destroying the software and all copies thereof.

4. Export Law Assurances. You agree and certify that neither the Software nor the documentation will be transferred or re-exported, directly or indirectly, into any country where such transfer or export is prohibited by the relevant governmental parties and regulations there under or will be used for any purpose prohibited by relevant government parties.

5. Warranty Disclaimer, Limitation of Damages and Remedies.
SubRosaSoft.com Inc. makes no warranty or representation, either expressed or implied, regarding the merchantability, quality, functionality, performance, or fitness of the compact disc, diskettes, manual or the information provided.

This software and manual are licensed “AS IS.” It is solely the responsibility of the consumer to determine the software’s suitability for a particular purpose or use. SubRosaSoft.com Inc. and anyone else who has been involved in the creation, production, delivery or support of the software, will in no event be liable for direct, indirect, special, consequential or incidental damages resulting from any defect, error or omission in the compact disc, diskettes, manual or software or from any other events including, but not limited to, any interruption of service, loss of business, loss of profits or good will, legal action or any other consequential damages. The user assumes all responsibility arising from the use of this software. SubRosaSoft.com Inc.'s liability for damages to you or others will in no event exceed the total amount paid by you for this software. In particular, SubRosaSoft.com Inc. shall have no liability for any data or programs stored by or used with SubRosaSoft.com Inc.’s software, including the costs of recovering such data or programs. SubRosaSoft.com Inc. will be neither responsible nor liable for any illegal use of its’ software. SubRosaSoft.com Inc. reserves the right to make corrections or improvements to the information provided and to the related software at any time, without notice.

SubRosaSoft.com Inc. will replace or repair defective distribution media or documentation at no charge, provided you return the item to be replaced with proof of purchase to SubRosaSoft.com Inc. during the 30-day period after purchase. ALL IMPLIED WARRANTIES ON THE MEDIA AND DOCUMENTATION, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO THIRTY (30) DAYS FROM THE DATE OF THE ORIGINAL RETAIL PURCHASE OF THIS PRODUCT. The warranty and remedies set forth above are exclusive and in lieu of all others, oral or written, expressed or implied. No SubRosaSoft.com Inc. dealer, representative, agent, or employee is authorized to make any modification, extension,

or addition to this warranty. Some States do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from State to State.

6. Government End-Users. If you are a Government end-user, this license of the software conveys only "RESTRICTED RIGHTS". This software was developed at private expense, and no part of it was developed with government funds. The software is a trade secret of SubRosaSoft.com Inc. for all purposes of the Freedom of Information Act, and is "commercial computer software" subject to limited utilization as provided in the contract between the vendor and the governmental entity, and in all respects is proprietary data belonging solely to SubRosaSoft.com Inc. Government personnel using the software, are hereby on notice that the use of this software is subject to restrictions that are the same as, or similar to, those specified above.

7. General. This license will be construed under the laws of the state of California, except for that body of law dealing with conflicts of laws, if obtained in the United States, or the laws of jurisdiction where obtained if obtained outside the United States. If any provision of this license is held by a court of competent jurisdiction to be contrary to law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this license will remain in full force and effect.

Complete Agreement. This license constitutes the entire agreement between the parties with respect to the use of the software and related documentation and supersedes all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter.

Copyright Notice

MacForensicsLab Web Agent Copyright Notice

SubRosaSoft.com Incorporated copyrights this software, the product design, and design concepts with all rights reserved. Your rights with regard to the software and manual are subject to the restrictions and limitations imposed by the copyright laws of the United States of America.

Under the copyright laws, neither the programs nor the manual may be copied, reproduced, translated, transmitted or reduced to any printed or electronic medium or to any machine-readable form, in whole or in part, without the written consent of SubRosaSoft.com Inc.

Trademarks

"MacForensicsLab Web Agent" is a trademark of SubRosaSoft.com Inc.

All other brand and product names are trademarks or registered trademarks of their respective holders.

