

SUBROSASOFT's
MacForensicsLab Social Agent



Copyright © 2010

The content of this document is wholly owned by SubRosaSoft Inc. and should not be copied either in part or in entirety without licence or expressed written permission of the copyright holder.

Trademarks

“MacForensicsLab Social Agent” is a trademark of SubRosaSoft.com, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

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	4
Overview of MacForensicsLab Social Agent.....	4
About MacForensicsLab Social Agent.....	4
System Requirements	5
Overview	5
Mac OS X Requirements.....	5
Registration Number	6
Uninstalling MacForensicsLab Social Agent.....	7
Elements of MacForensicsLab Social Agent	9
Social networks	9
The 'Statistics' area	10
Running MacForensicsLab Social Agent.....	10
Configuring MacForensicsLab Social Agent.....	10
Running a search.....	11
Reviewing search results.....	11
Getting Help and Technical Support	12
Finding Help within MacForensicsLab Social Agent.....	12
On the Web.....	12
Technical Support.....	12
Comments and Questions	13
Company Address.....	13
End User's License Agreement (EULA)	14
End Users License Agreement	14
EULA	14
Copyright Notice	16
MacForensicsLab Social Agent Copyright Notice	16
Trademarks	17

Overview

Overview of MacForensicsLab Social Agent

This section provides an overview of MacForensicsLab Social Agent and its features, functionality and design.

About MacForensicsLab Social Agent

Welcome to MacForensicsLab Social 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 Social Agent allows forensics examiners and detectives to quickly search a suspects Apple Safari internet cache for the presence of information related to various social networking sites. Screenshots of social network sites the user visited are displayed once identified and may contain valuable evidence for an investigator. Social Agent only works on Macs running Safari. Other browsers are not currently supported.

System Requirements

Overview

This section covers the basic and recommended system requirements for successfully running MacForensicsLab Social 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 Social 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

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 Social 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 Social 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 Social 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.

Note: The software can be run directly from the special Flash Key based version.

Installation

Having decompressed the folder, simply drag and drop Social Agent where you would like the application to reside and be run from. Investigators may want to copy Social Agent to a USB flash drive to allow them to run the application on a suspect's Mac.

Uninstalling MacForensicsLab Social Agent

MacForensicsLab Social Agent is a completely self-contained application and requires no special functionality to uninstall it. The procedure to uninstall MacForensicsLab Social Agent is to navigate to the application, highlight MacForensicsLab Agent and either drag and drop it into the Trash.

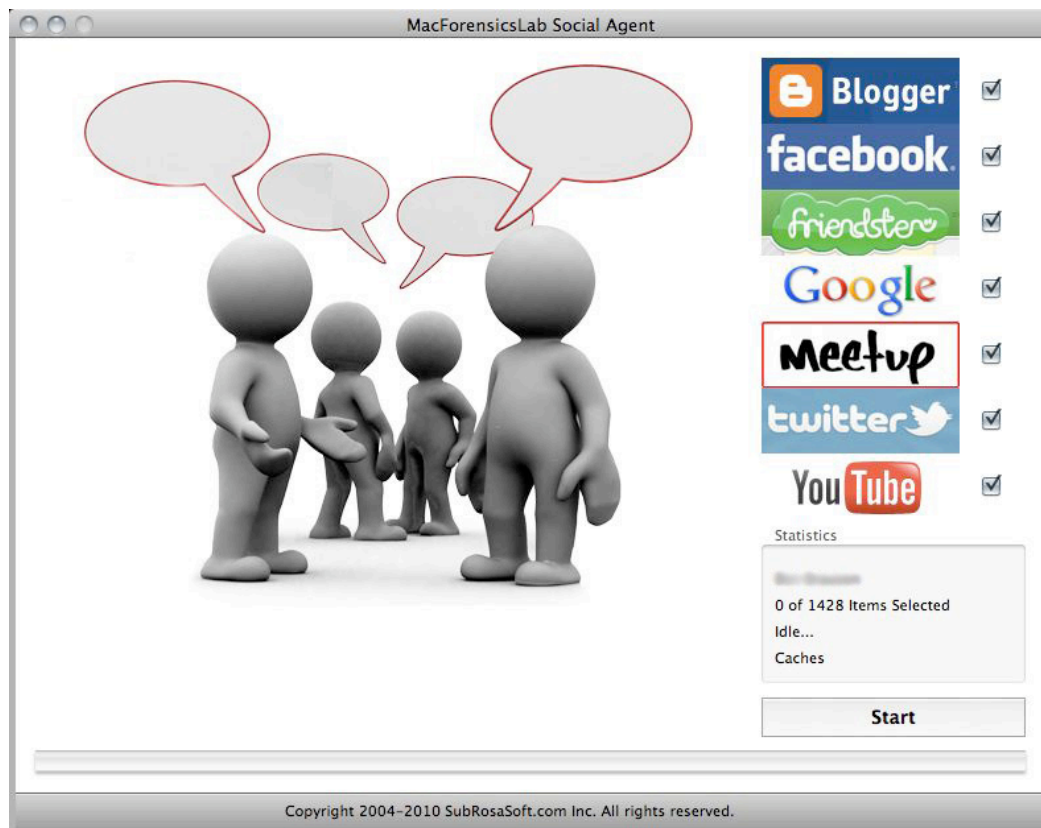
Initial Setup

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 Social Agent

Designed for non-technical personnel, Social Agent is extremely easy to use; there is no rebooting, troubleshooting or complex interfaces. It quickly searches for information related to a number of social network sites. By quickly providing images relevant to an investigator's interests, MacForensicsLab Social Agent is an invaluable tool to all law enforcement agencies.

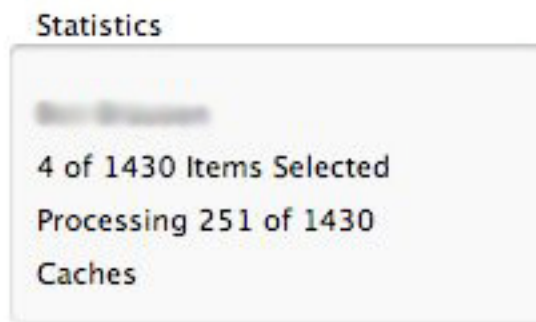


Social networks

MacForensicsLab Social Agent has the ability to search a number of popular social networks for information that may be valuable to an investigation. These networks are shown in Social Agent and include; Blogger, Facebook, Friendster, Google, Meetup, Twitter, and YouTube. Each network has a checkbox next to it's name to allow the investigator to select the networks Social Agent will search for. By default, all networks are selected. Simply un-check the box next to a network's name to skip searching for that network. Check it to include the network in the search.

The 'Statistics' area

The statistics area shows various information about the search.



The first thing shown is the username of the account that will be searched. This is the name of the account the user is currently logged into. SubRosaSoft.com Inc. suggests investigators either purchase Social Agent on a USB thumb drive or install the application on their own thumb drive so they may attach the drive to a suspect machine and run Social Agent on the active system.

The next line shows the number of items found in the Safari cache. As a search is run, this statistic will show the number of files found out of the total number of files.

The third line shows the number of files that are being processed out of the total number of files.

Running MacForensicsLab Social Agent

Configuring MacForensicsLab Social Agent

The first step in configuring Social Agent is to select the social networks to be searched for. By default, all networks are selected. To de-select a network and remove it from the search, simply uncheck the box next to its name. To select a network, check the corresponding box.

Running a search

Once the user has selected the social networks they wish to search for, click the **Start** button. This will display a save dialog. Select the folder you wish to save the search results to and click **Choose**. The search will then begin. Search statistics will be shown in the **Statistics** area and images of the social networks will be shown as they are found in the main window.

Reviewing search results

Name	Date Modified
▶ folder blogger_thumbnail	Today, 7:33 PM
▶ folder facebook	Today, 7:32 PM
▶ folder facebook_thumbnail	Today, 7:32 PM
▶ folder google	Today, 7:31 PM
document icon Log.txt	Today, 7:33 PM
▶ folder meetup	Today, 7:31 PM
▶ folder meetup_thumbnail	Today, 7:31 PM
▶ folder youtube_thumbnail	Today, 7:33 PM

When the search has completed, the folder containing the search results it opened in the Finder. This folder's name contains the username of the account that was scanned along with the time and data of the scan. Within this folder are subfolders for each social network found. Some networks will also have a folder containing thumbnails of the images. These folders have the name of the social network with **_thumbnail** appended to the end of the name. Within each folder are the images found during the scan. These images are the screen shot images cached by Safari. Hash values, source and destination information for each image are stored in the search folder in the text file titled **Log.txt**.

Getting Help and Technical Support

Finding Help within MacForensicsLab Social 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 Social 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 Social Agent™ software only on a SINGLE computer at any one time. You may only use the MacForensicsLab Social 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 Social 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.

© Copyright 2010 SubRosaSoft.com Inc. All Rights Reserved

Trademarks

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

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