Chromensics

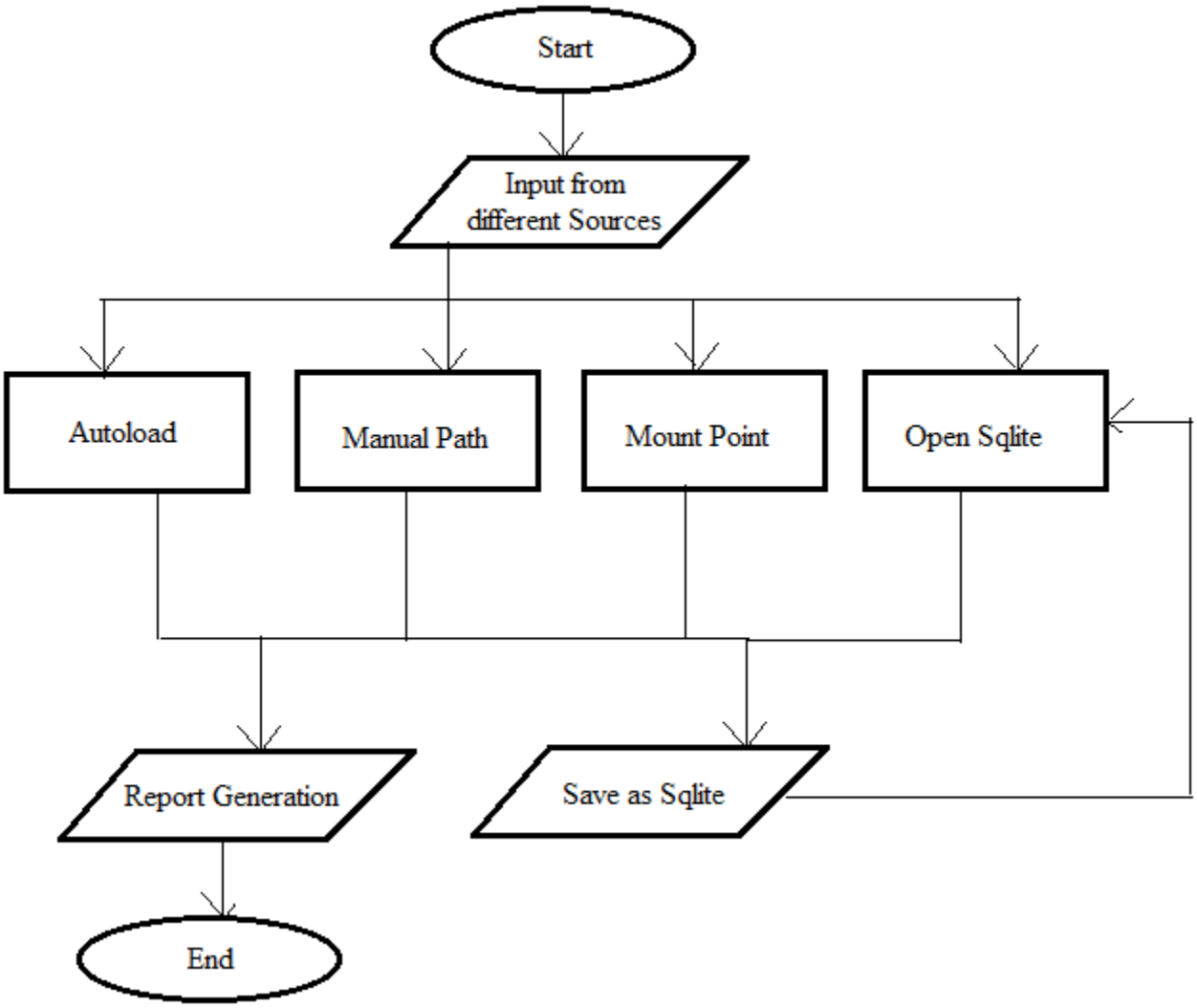
Google Chrome Forensics Tool

User Manual

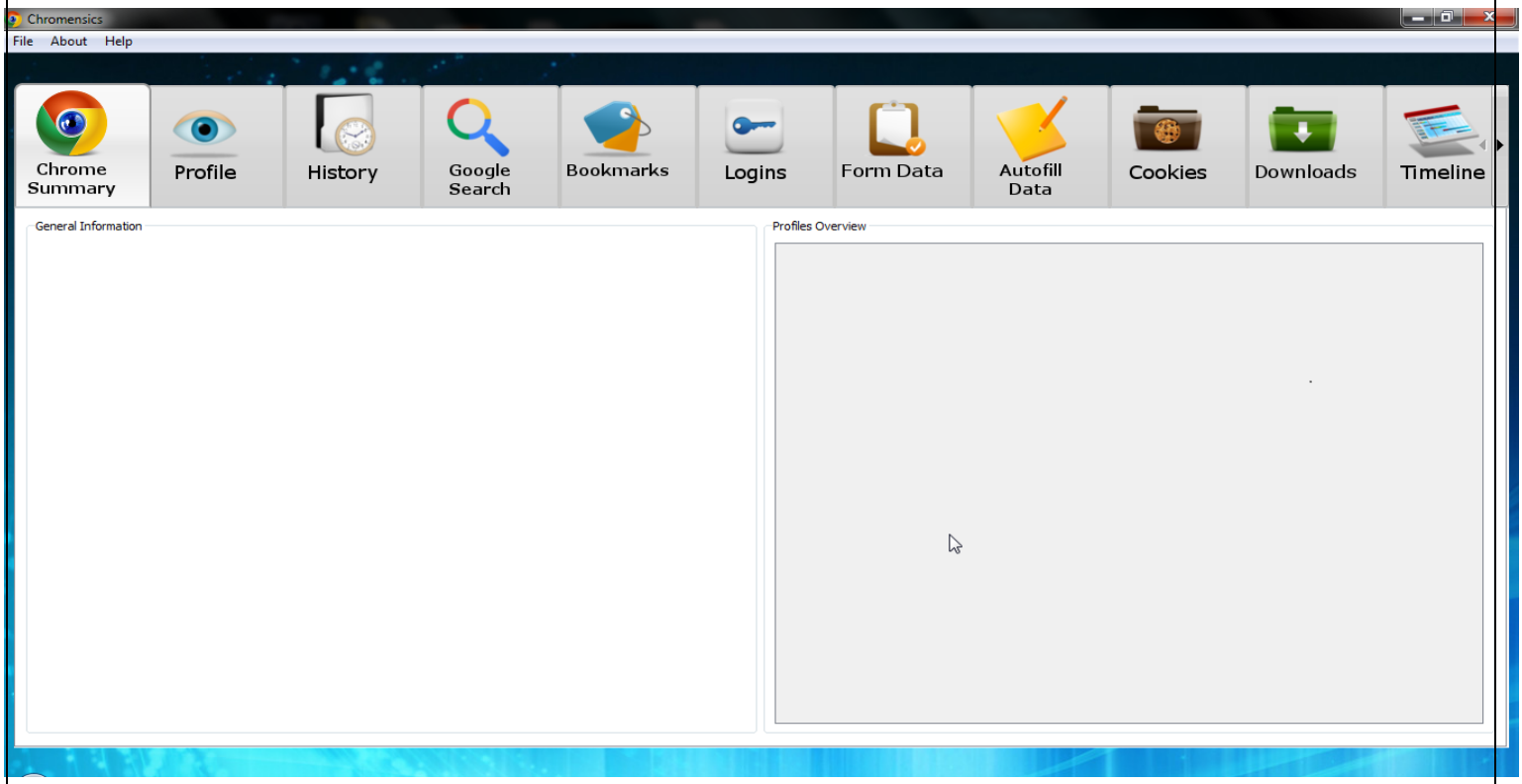
By Nishant Grover

The **Chromensics** tool is developed to read all information from chrome browser directory and present it to user, in easy readable tabular format which can be explored in descent interface without running the chrome browser. The tool will also allow you retrieve information from other chrome installation brought from different machine for analyzing. The acquired artifacts can be exported in PDF report to present it in court of law or to superiors.

Flow Chart

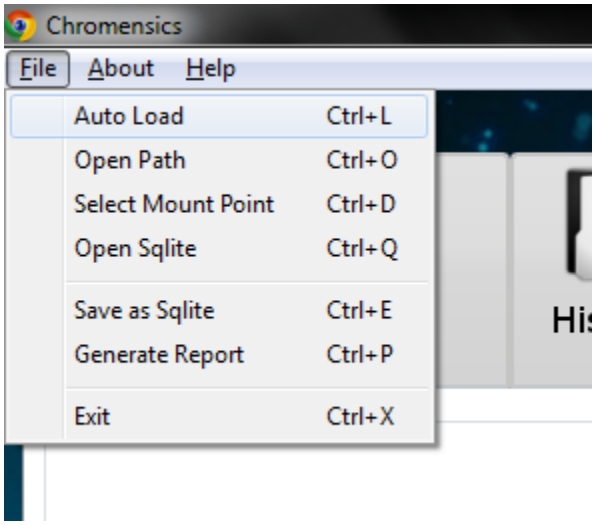


1. How to Start

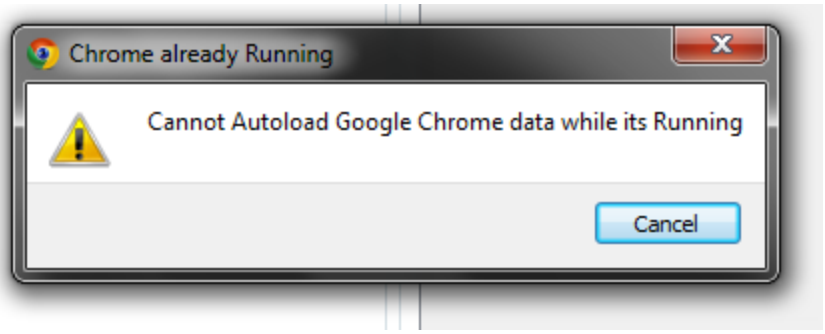


This is the main GUI(Graphical User Interface) of Tool, Start by Clicking the File Menu on the Top or by pressing appropriate keyboard Keys.

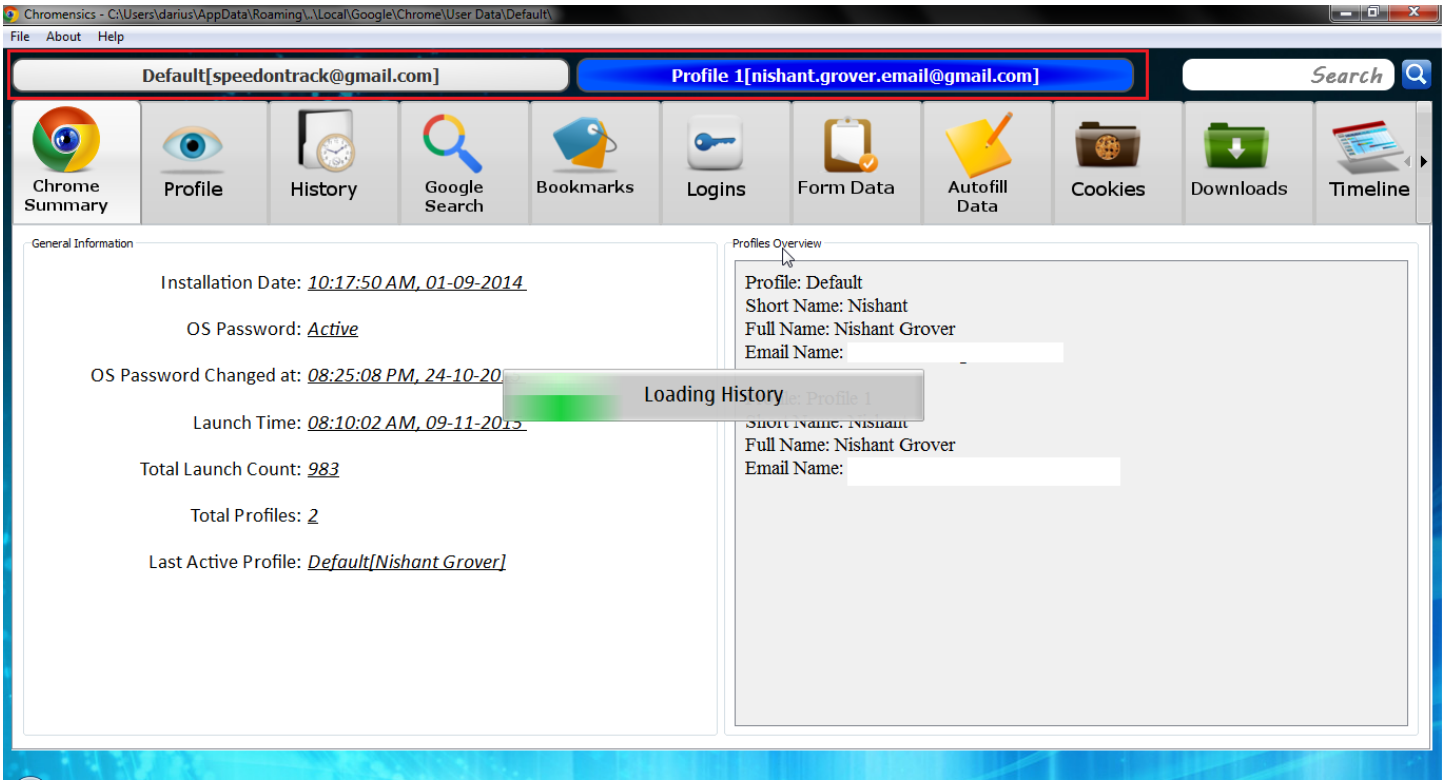
2. Autoload(CTRL+L)



Autoload works by loading the installation of chrome inside System, If your chrome installation is already going on, it will not work. You need to close Google chrome for this option to work. If even after closing it doesn't work, make sure chrome.exe is not running in processes, you can check processes from Task Manager by Pressing CTRL+ALT+DEL.

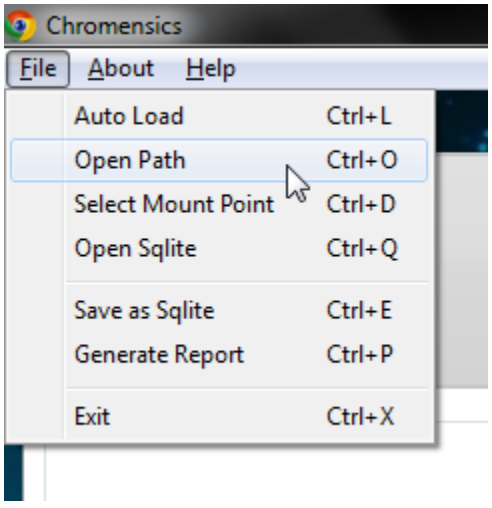


After clicking the menu option, data will be loaded automatically. The Red Marked Area shows different profiles found.



The data will be loaded in no time, a progressbar is visible for progress. Now you can browse all Data in each tab.

3. Manual Path(CTRL+O)

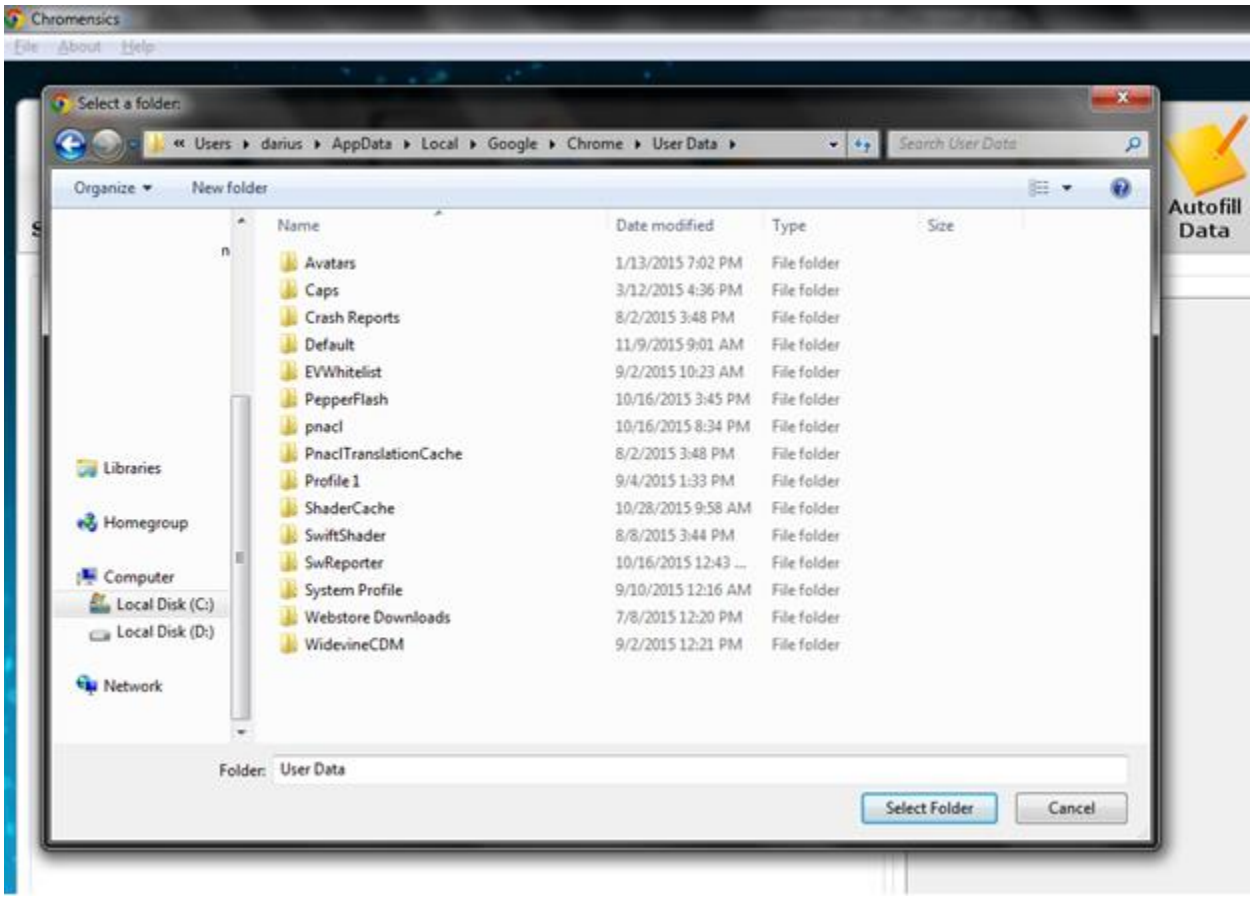


Through this option, any chrome installation can be loaded in chromensics, whether it belongs your system or it is brought from other system (can be suspect or person under analysis).

The Default Path for Chrome Installation is(Windows Machines Only)

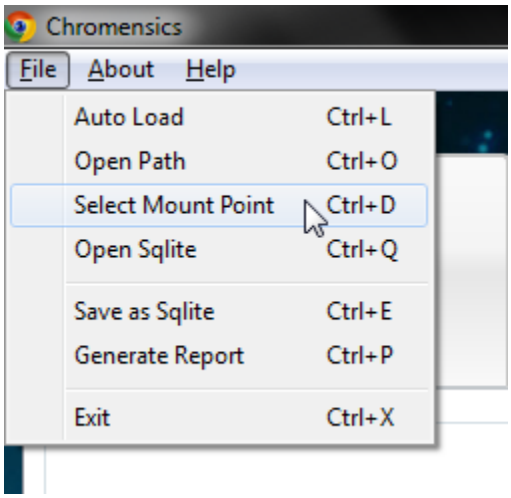
Windows 7/8/10: C:\Users\[userdir]\AppData\Local\Google\Chrome\User Data

Windows XP: C:\Documents and Settings\[userdir]\Local Settings\Application Data\Google\Chrome\User Data\

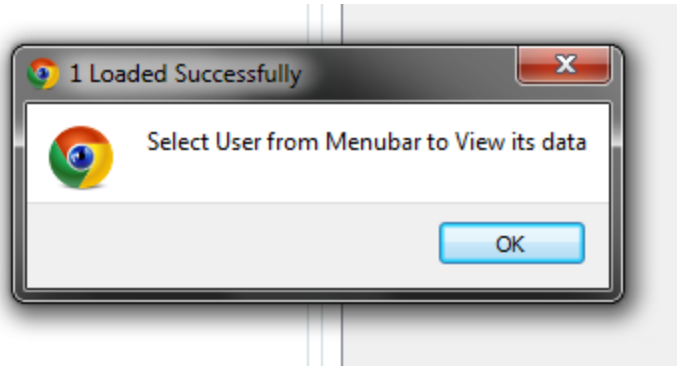


You can copy **User Data** Directory from other systems and locate them in Manual Path for loading in Chromensics.

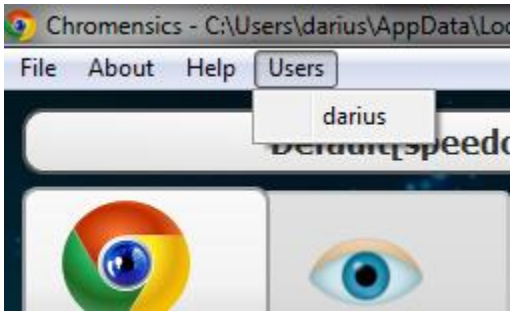
4. **Load Mount Point(CTRL+D)**



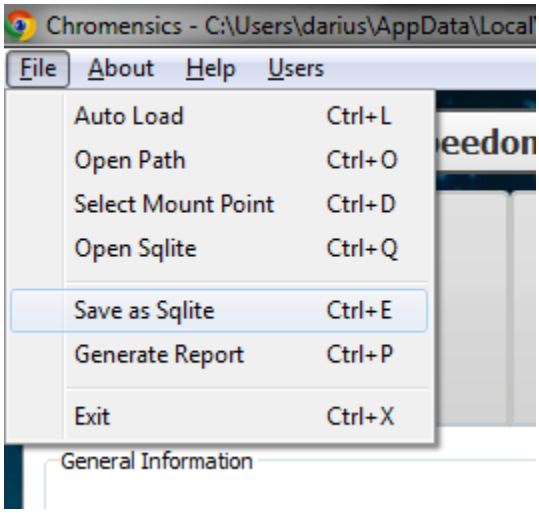
With this Option you can locate Mount Point or Drive where Evidence is Mounted at. After Selection a popup will appear



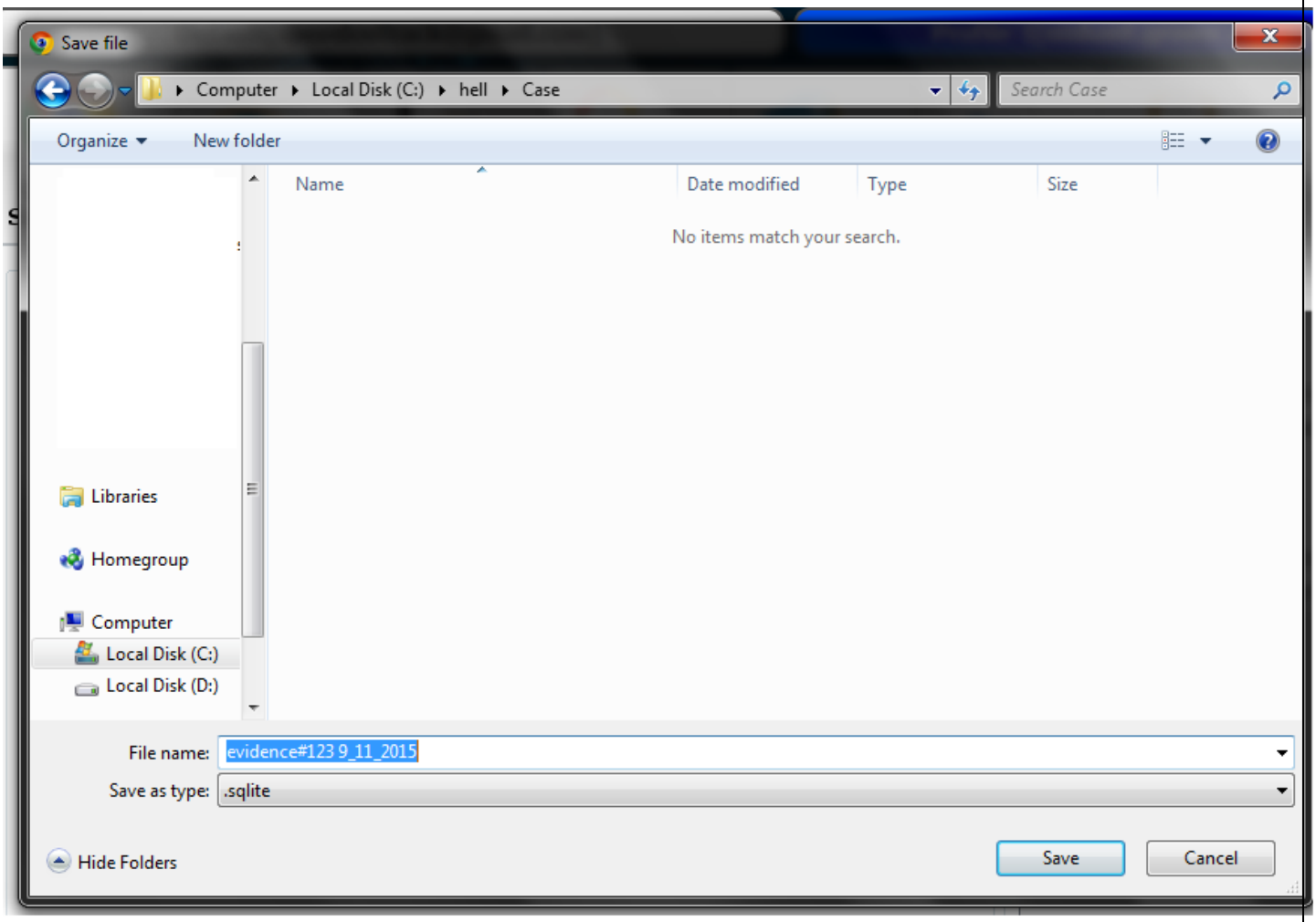
And now you can select User in Menubar where chrome installation is found to load data from it.



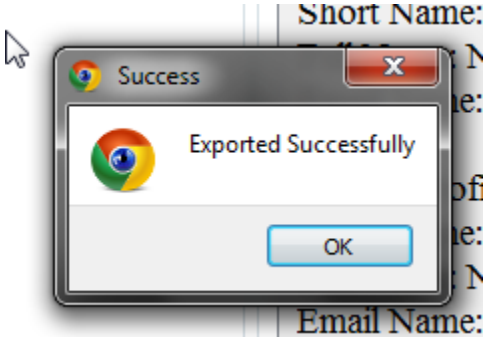
5. **Export Sqlite(CTRL+E)**



This option will allow you to export all the data acquired into a single .sqlite file which can be transferred over the network for sharing with superiors or colleagues for analysis.



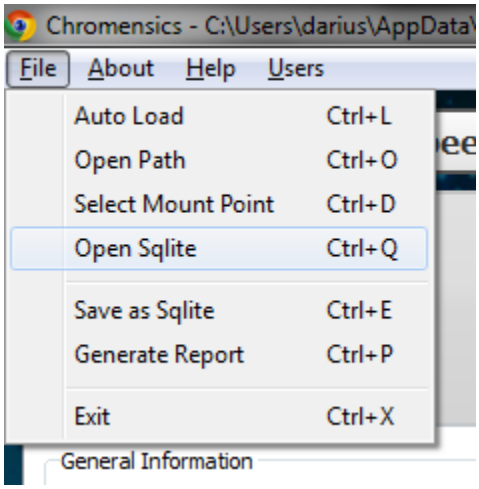
Type a File Name and Click Save



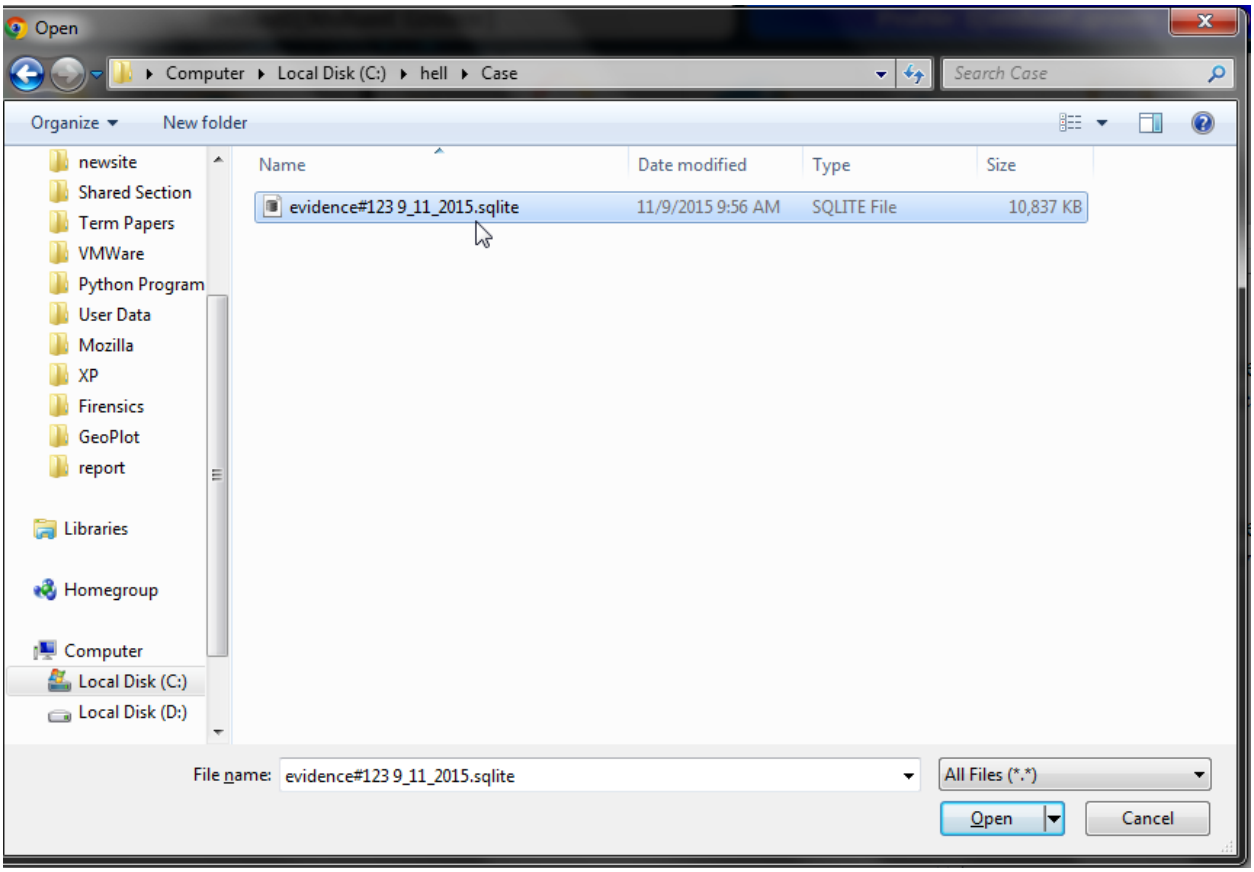
A Popup will appear after exporting, with Success Message.

Note: Save as Sqlite will Export selected active profile only.

6. **Import Sqlite(CTRL+Q)**

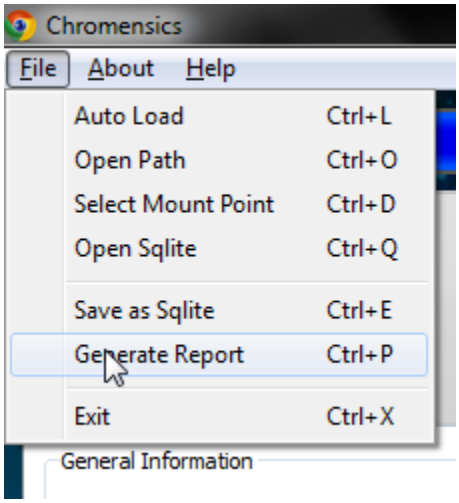


This Option will allow you to load data from .sqlite from created in "**Save as Sqlite**".

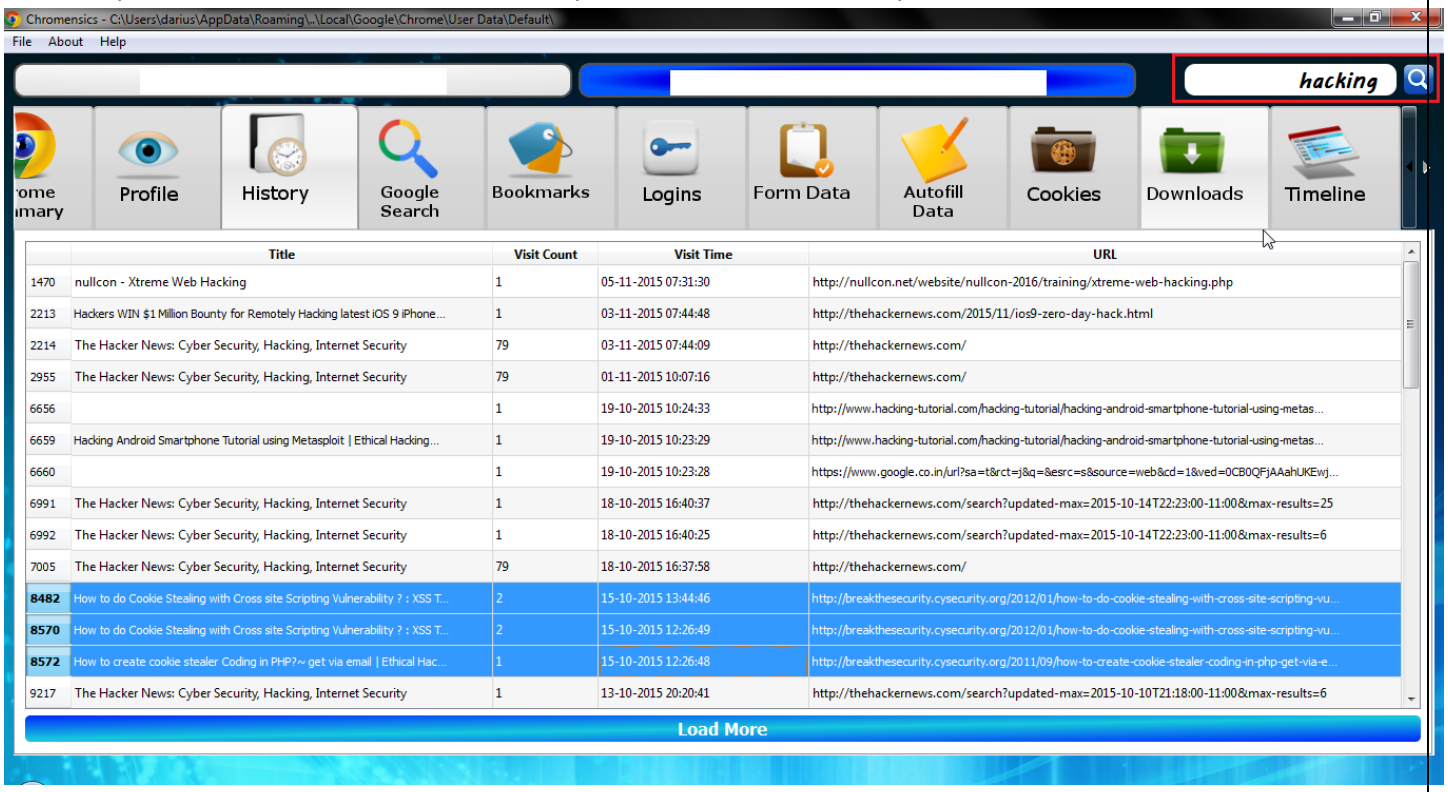


After selecting the .sqlite file, data will be loaded from it for analysis.

7. Report Generation(CTRL+P)



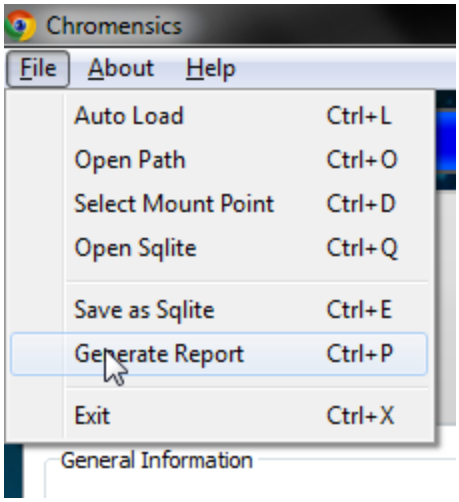
The data loaded from chrome can be analyzed to generate a forensic report. Only the selected rows from each tab can be exported into PDF. You can use Search Option to find the related keywords faster.



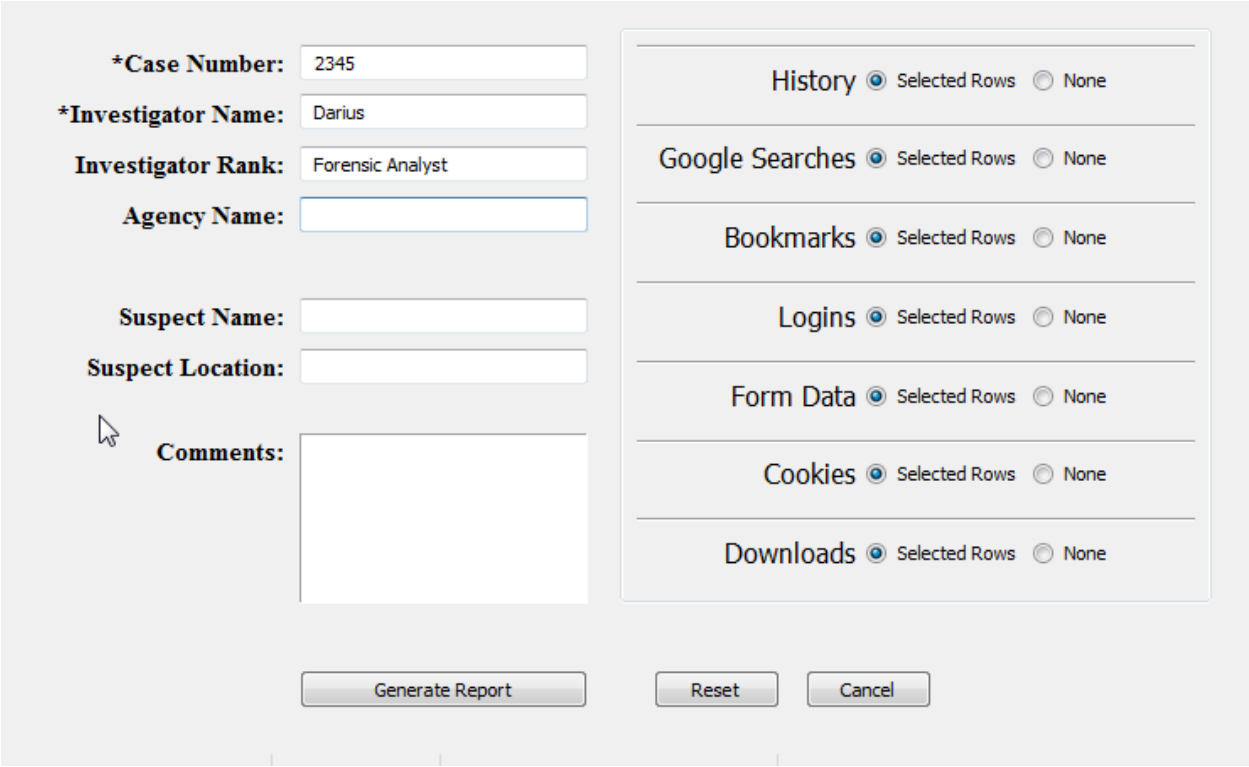
	Title	Visit Count	Visit Time	URL
1470	nullcon - Xtreme Web Hacking	1	05-11-2015 07:31:30	http://nullcon.net/website/nullcon-2016/training/xtreme-web-hacking.php
2213	Hackers WIN $1 Million Bounty for Remotely Hacking latest iOS 9 iPhone...	1	03-11-2015 07:44:48	http://thehackernews.com/2015/11/ios9-zero-day-hack.html
2214	The Hacker News: Cyber Security, Hacking, Internet Security	79	03-11-2015 07:44:09	http://thehackernews.com/
2955	The Hacker News: Cyber Security, Hacking, Internet Security	79	01-11-2015 10:07:16	http://thehackernews.com/
6656		1	19-10-2015 10:24:33	http://www.hacking-tutorial.com/hacking-tutorial/hacking-android-smartphone-tutorial-using-metas...
6659	Hacking Android Smartphone Tutorial using Metasploit | Ethical Hacking...	1	19-10-2015 10:23:29	http://www.hacking-tutorial.com/hacking-tutorial/hacking-android-smartphone-tutorial-using-metas...
6660		1	19-10-2015 10:23:28	https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB0QFjAAahUKEwj...
6991	The Hacker News: Cyber Security, Hacking, Internet Security	1	18-10-2015 16:40:37	http://thehackernews.com/search?updated-max=2015-10-14T22:23:00-11:00&max-results=25
6992	The Hacker News: Cyber Security, Hacking, Internet Security	1	18-10-2015 16:40:25	http://thehackernews.com/search?updated-max=2015-10-14T22:23:00-11:00&max-results=6
7005	The Hacker News: Cyber Security, Hacking, Internet Security	79	18-10-2015 16:37:58	http://thehackernews.com/
8482	How to do Cookie Stealing with Cross site Scripting Vulnerability ? : XSS T...	2	15-10-2015 13:44:46	http://breakthesecurity.cysecurity.org/2012/01/how-to-do-cookie-stealing-with-cross-site-scripting-vu...
8570	How to do Cookie Stealing with Cross site Scripting Vulnerability ? : XSS T...	2	15-10-2015 12:26:49	http://breakthesecurity.cysecurity.org/2012/01/how-to-do-cookie-stealing-with-cross-site-scripting-vu...
8572	How to create cookie stealer Coding in PHP?~ get via email | Ethical Hac...	1	15-10-2015 12:26:48	http://breakthesecurity.cysecurity.org/2011/09/how-to-create-cookie-stealer-coding-in-php-get-via-e...
9217	The Hacker News: Cyber Security, Hacking, Internet Security	1	13-10-2015 20:20:41	http://thehackernews.com/search?updated-max=2015-10-10T21:18:00-11:00&max-results=6

The Red Box in top right corner display the search box. For Example, Above Records are selected as user was intending to do XSS attack and was learning how to do it.

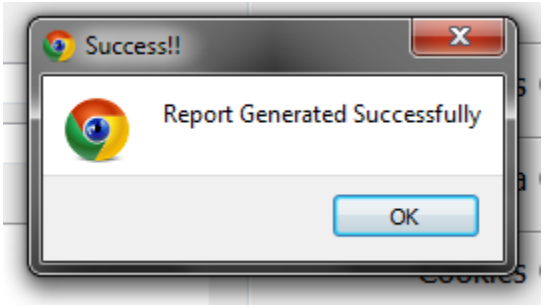
Note: Searching will be done in active tab only.



After selecting the records that you want to show in report from appropriate tabs, Click on Generate Report



Fill up the displayed dialog box and click generate to create Report.



A popup will confirm its creation.

You can now check the report for records u have exported into.