

# eForensics

M a g a z i n e

**Network**

VOL.2NO.14

# Internet Browsers Forensics

70+  
PAGES



**COMPARISON OF 5 TOP BROWSERS:  
FIND THE ONE STEP BY STEP**

**CHROME FORENSICS – HOW TO TRACE  
YOUR INTERNET ACCESS BEHAVIOR**

**HOW TO AVOID SECURITY FLAWS IN APPS  
USING IOS WEB VIEWS**

**GOOGLE CHROME – THE FUTURE OF WEB  
COMPUTING**

**SECPOINT CLOUD PENETRATOR**

# DATA SECURITY

## Computer Forensics Experts

### Computer Forensics Services

We are prepared to attend the situation urgency supporting your needs and delivering our consulting solutions considering our worldwide cybercrime knowledge base by:

- Dispute support services
- Evidence Identify and Collection
- Evidence Analysis and Reporting
- Device analysis as: Computers, Smartphones, Tablets, Network, Printers, even Games Consoles...

### Computer Forensics Training

Get in touch enjoying our cases applying methodologies and tools resolving a real forensic case in 40 hours. At last you will be submitted by a certification test (DSFE) proofing your skills.



R. Eça de Queiroz, 682 – Vila Mariana

São Paulo, S.P. 04011-033 - Brazil

Phone: +55 11 5011-7807

E-mail: [datasecurity@datasecurity.com.br](mailto:datasecurity@datasecurity.com.br)

 [facebook.com/data.secur.face](https://facebook.com/data.secur.face)



[@datasecurity1](https://twitter.com/datasecurity1)





*\*pending final confirmation*

**Confirmed Speakers:**

- Mr. Noboru Nakatani**, Executive Director, **INTERPOL Global Complex for Innovation**
- Mr. Anwer Yussoff**, Head of Innovation and Commercialisation, **CyberSecurity Malaysia**
- Mr. Mohd Zabri Adil Bin Talib**, Head of Digital Forensics, **CyberSecurity Malaysia**
- Dr. Mingju Jumaan**, Director, **Sabah State Computer Services Department, Malaysia**
- Mr. Lauri Korts-Pärn**, CTO, **Cyber Defense Institute, Japan**
- Mr. Jack YS Lin**, Information Security Analyst, **JPCERT, Japan**
- Mr. Roberto Panganiban**, System Administrator, **Philippines News Agency**
- Mr. Budi Rahardjo**, Chairman, **ID-CERT , Indonesia \***
- Mr. Matthew Gartenberg**, Chief Legal Officer, **Centre for Strategic Cyberspace + Security Science \***
- Mr. Adli Wahid**, Manager, Cyber Security / MUFG-CERT, **Bank of Tokyo**
- Mr. Kislay Chaudhary**, Director and Senior Information Security Analyst, **Indian Cyber Army**
- Mr. Leo Dofiles**, Computer Crime Investigator/Computer & Cellphone Forensics Planner, **National Police, Philippine**
- Mr. Jairam Ramesh**, IT Infrastructure, **International Multilateral Partnership Against Cyber Threats (IMPACT), Malaysia \***
- Mr. Ng Kang Siong**, Principle Researcher, **MIMOS Berhad, Malaysia**

**Organised by:**



**Sponsored by:**



**Supported by:**



**Media Partner:**



**Editors:**

Maria Ocioszyńska  
maria.ocioszynska@software.com.pl

**Betatesters/Proofreaders:**

Gabriele Biondo, Jan-Tilo Kirchoff,  
Salvatore Fiorillo, William Poole, Kamal,  
Alex Rams, M1ndI3ss, Robert E. Vanamann  
M.S., Dr. Db Karron, Indigo Larson

**Senior Consultant/Publisher:**

Paweł Marciniak

**CEO:** Ewa Dudzic

ewa.dudzic@software.com.pl

**Production Director:** Andrzej Kuca

andrzej.kuca@software.com.pl

**Marketing Director:** Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

**Art Director:** Ireneusz Pogroszewski

ireneusz.pogroszewski@software.com.pl

**DTP:** Ireneusz Pogroszewski

**Publisher:** Hakin9 Media Sp. z o.o. SK

02-676 Warszawa, ul. Postępu 17D

Phone: 1 917 338 3631

www.eforensicsmag.com

**DISCLAIMER!**

*The techniques described in our articles  
may only be used in private, local net-  
works. The editors hold no responsibility  
for misuse of the presented techniques or  
consequent data loss.*

## Dear Readers!

Welcome to the September issue of eForensics Network devoted to Internet Browsers Forensics. We are trying to present our original ideas in four lines – Database, Computer, Network and Mobile. I encourage you to get to know with 'Internet Browsers Forensics' content and have fantastic time with a good piece of reading. For sure you will be satisfied with both specialistic and introductory articles prepared by our experienced experts.

A web browser is a software application for retrieving, presenting and traversing information resources on the World Wide Web. Although browsers are primarily intended to use the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems. The major web browsers are Google Chrome, Mozilla Firefox, Internet Explorer, Opera, and Safari.

Most browsers support HTTP Secure and offer quick and easy ways to delete the web cache, cookies, and browsing history. But do we know the advantages and disadvantages of our browser's security. Which internet browser is the best? You will definitely know the answer after reading this edition!

I encourage you to read this eForensics Network edition. Taking advantage of this publication I would like to invite you to co operation and encourage you to give a feedback concerning our work. Please follow us on Facebook and Twitter, where you can find the latest news about our magazine and great comments. You can also suggest what topics you would like us to cover and what tools you would like to know. Do you like our magazine? Click LIKE IT! and SHARE IT! We appreciate your every comment!

Enjoy reading!  
Maria Ocioszyńska  
eForensics Team

# 08

## COMPARISON OF 5 TOP BROWSERS: FIND THE ONE STEP BY STEP

by Terry Tang

Browser has already been a necessary tool for everyone in surfing the internet nowadays. To name the most common ones: Internet Explorer, Firefox, Google Chrome, Safari, Opera. Other browsers are generally developed based on the cores of the five above, which makes them already included in the list.

# 16

## CLOUD

by Rick Clark

Cloud collections, cloud storage, collections through the cloud, cloud, cloud....cloud. Cloud is such a simple term, but has many meanings, implications and applications to the forensic and legal industry. I believe the growing confusion in the legal space is due to the need to categorize the applications of cloud offerings and how to best utilize them.

# 22

## GOOGLE CHROME - THE FUTURE OF WEB COMPUTING

by John Blossom

By many estimates the browser wars are over, and Google Chrome has won. Yet although Google Chrome has become a broadly used tool for accessing and publishing Web information, the full impact of Chrome is just beginning to come into focus for many people. What is Chrome all about, and where is it taking us? John Blossom, President of Shore Communications, Inc., is a leading content and technology industry analyst who sees the evolution of Google Chrome as a major factor in the development of secure, Web-centered computing services.

# 30

## GOOGLE CHROME FORENSICS

by Krystina Horvath

In this article, you will learn about the technical forensic processing of the Google Chrome web browser as used on Linux and Windows operating systems. Privacy issues concerning Chrome and how they are beneficial to forensic investigators will also be discussed.

# 36

## CHROME FORENSICS - HOW TO TRACE YOUR INTERNET ACCESS BEHAVIOR

by Nichols Jasper

This article describes computer forensic procedures for discovering Internet Browsing habits, and compiling computer user profiles. This paper suggests useful information regarding the type of information, and how Chrome defaults' directories are used, and what kind of browsing information may be recovered from computers. Simplifying collection and some reporting tools are described.



cutting through complexity

# Are you prepared?

[kpmg.ca/forensic](http://kpmg.ca/forensic)

# INTRUSION

ATTACK • THREAT • CYBER SECURITY

TECHNOLOGY • CORPORATE

ELECTRONIC • INFORMATION • COMPLEXITY

# DATA ANALYTICS

RISK • INFORMATION • TECHNOLOGY

# DATA RECOVERY

COMPLEXITY • ELECTRONIC • INFORMATION

# FORENSICS

DATABASE • ELECTRONIC • CONTROL

# INTELLIGENCE

INFORMATION • RISK • TECHNOLOGY

# eDISCOVERY

COMPLEXITY • THREAT • INTELLIGENCE

# INVESTIGATIONS

# TECHNOLOGY

COMPLEXITY • THREAT • DATABASE

INTELLIGENCE • PROTECTION

# CORPORATE

© 2013 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

44

### SAFARI BROWSER FORENSICS ARTIFACTS ANALYSIS

by Mr. Darsh Patel, Dr. M. S. Dahiya, Dr. J. M. Vyas

Apple Safari is the default web browser on Macintosh Systems. The following are key Safari plist files which can give lots of artifacts related with the browser usage and forensic evidences.

48

### BROWSER FORENSICS ON MACS: SAFARI!

by John Reed

What is browser forensics? Most folks probably have no idea what it is or why they need it. In a nutshell forensics will enable you to see what has been going on in your browser on your system or a browser on another system. What sites have been visited, how that system is being tracked, how often sites are seen and what content has been downloaded to that machine. In the last 10 years the Mac and it's siblings (iPhone, iPad) have made explosive growth in the enterprise market, from IT to sales and marketing Macs have become present enough that sys admins have to pay attention to them and make sure that the Mac and it's users follow the rules, and subsequently be able to find out when they don't.

50

### HOW TO AVOID SECURITY FLAWS IN APPS USING IOS WEB VIEWS

by Maria Davidenko

iOS is considered the most secure touch OS because of its closed nature. However, that doesn't mean that there is no place to worry about your data safety and integrity, or, to be more precise, about your user's data safety. There are plenty of tools developers get with the iOS SDK to provide a great user experience within their apps, there are, however, few tools you may use to provide safe Internet browsing within your apps. UIWebView is one of them.

54

### CYBERSECURITY IN ROMANIA

by Dr. Laurent Chrzanovski

Some may say it is another conference just to surf on one of the hottest issues of our times. Some may think too many NGOs are dealing with the same subject and sharing the same ambitions. Probably both presumptions are right. And yet they do not fit the challenge we are trying to take on.

58

### WEB BROWSER FORENSICS: Q&A WITH CCL-FORENSICS

by Indigo Larson

CCL was founded as an independent IT consultancy in 1986 by Andrew Krauze, the company's managing director, offering experienced and independent consultancy to ensure IT effectively supports business objectives. This forms the bedrock of CCL – our services and solutions are backed up by our team of highly knowledgeable consultants with years of industry experience behind them.

60

### THE NATIONAL RETAIL CRIME CONFERENCE (NRCC) – DUBLIN 2013

by Karen McNavin

The National Retail Crime Conference (NRCC) is delighted to announce its inaugural event launching on the 16th October 2013 in the Citywest Conference Centre, Dublin. This conference will offer Retail/Loss Prevention and Security professionals the opportunity to come together for networking, information sharing and to gain intelligence on crime within the retail industry.

62

### SECPOINT CLOUD PENETRATOR

by Casey Parman

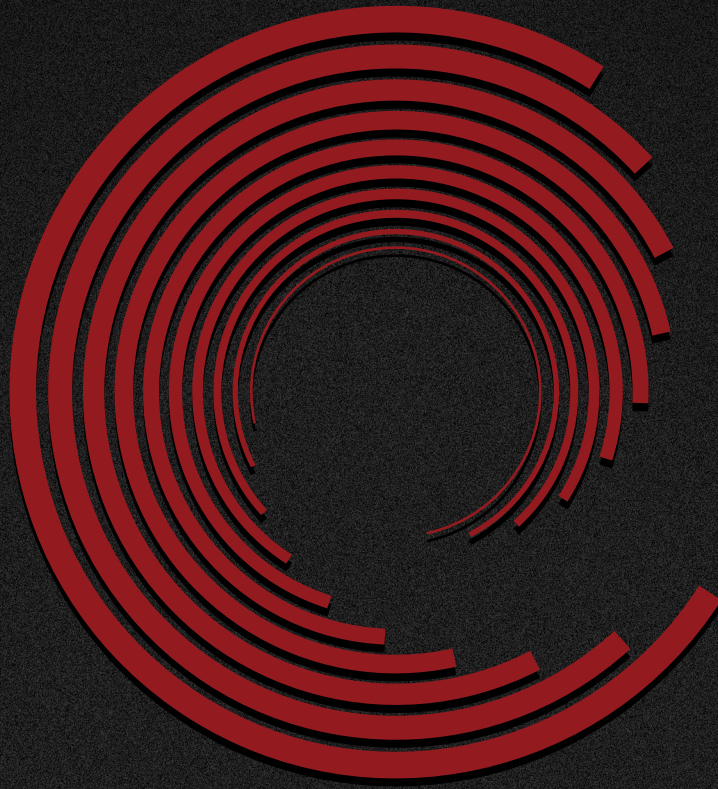
Network security has rapidly become a significant part of Information Technology Infrastructure consisting of policies to prevent unauthorized access to data in a network. Without a strong security plan companies find themselves vulnerable to intrusion without any knowledge of a threat. The best solution is to hire a Security Specialist but this isn't always applicable; many companies can't afford to pay a specialist, or when they can, can they be sure their company is truly protected?

66

### LAWTECH EUROPE CONGRESS COLLABORATES WITH LEADING TECHNOLOGY PROVIDERS CISCO AND ALUCID FOR EFFICIENT VIDEO STREAMING AND SECURE AUTHENTICATION

by LawTech Europe Congress Collaborates

For the first time, LTEC participants can attend its annual event via live streaming video with the support of Cisco TelePresence®. In addition, all LTEC delegates will be provided secure authentication keys compliments of ALUCID®.



# **Remediant**

## **Security You Trust**

**Counter-Espionage • APT Remediation  
Cybersecurity Strategy**

**[www.remediant.com](http://www.remediant.com) • 877.437.9947**

# COMPARISON OF 5 TOP BROWSERS:

## FIND THE ONE STEP BY STEP

by **Terry Tang**; Translator: **Kim Paix**

Browser has already been a necessary tool for everyone in surfing the internet nowadays. To name the most common ones: Internet Explorer, Firefox, Google Chrome, Safari, Opera. Other browsers are generally developed based on the cores of the five above, which makes them already included in the list.

### What you will learn:

- Development background of each browser.
- Advantages & Disadvantages of each browser.
- All-around Performance Comparison in: startup speed, webpage loading speed, memory usage, security, compatibility, Extensions.

### What you should know:

- Familiarity with basic usage of browsers

Which one should we users choose, from so many candidates, to best suite our needs? To make the choice an easier one to make, in the following content, we will make a rough introduction to each of the 5 browsers mentioned above and compare certain benchmarks that users care most. Let's find the One step by step.

### INTERNET EXPLORER

Born in 1995 by Microsoft, Internet Explorer is an old brother among browsers and it still takes the first place in market share today. It uses Trident as layout engine.

We have witnessed the development history of common IE versions from IE6, IE7, IE8, IE9, IE10, to IE11, which has just been released and has less users. Among them, IE6 is gradually vanishing and only seen on old

computers of low configuration. IE7 is not commonly seen today, as it's not a default built-in browser of any Windows OS and it's the first IE browser to support Multi-Tab browsing, which caused its problems of numerous bugs and mediocre performance and therefore low coverage in market share. Most users simply used it for trying an upgrade from IE6. IE8 is the built-in browser of Windows7 and has better performance than IE7 both in functionality and compatibility. IE9, a built-in in Windows7 SP1, took a leap from IE 8 and now has the most market share among all IE versions. IE10 is the built-in browser in Windows8 and also has improved itself a lot from the previous version. Within less than 1 year from the release of IE10 had Microsoft launched IE11, which was aiming at touch screen using experience and speeding. It also focuses



at advancing internet standard support and browser using experience, which makes it a preference more to screen touch devices like tablet PCs. From 9 on, IE starts supporting hardware speedup, i.e. using GPU to speedup webpage display. However, this feature is only supported in Windows7, while the other 4 brands of browsers can support hardware speedup completely.

**ADVANTAGES**

The most notable advantage of IE is its excellent compatibility. Almost all types of webpage displays are compatible with IE; some online payment and bank systems only support IE operations. The second advantage, obviously, is that IE needs no additional download & install since it's installed while Windows operating system is being installed.

**DISADVANTAGES**

It's relatively slow when opening webpages. This has already been improved a lot in IE10 and IE11 but still has a long way to go compared to Chrome.

Previous versions including IE10 all used to have lost response sometimes and they are easy to collapse, a stubborn problem to which a solution will be discussed later. IE11 is not found to have lost response for the moment. Its security is not that good, which has caused a relatively high possibility to get affected. This has been improved since IE9. Finally, it devours memory, which will be analyzed in the following paragraphs.

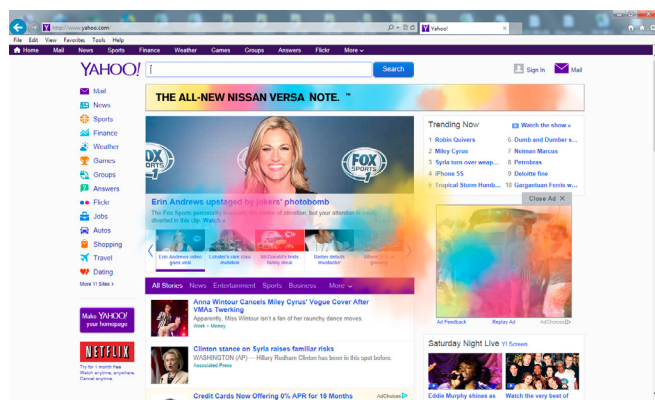


Figure 1. Destination site opened in IE

**FIREFOX**

Mozilla Firefox is a simple open source webpage browser with high extensibility. With its name changed from originally Phoenix to Mozilla Firebird and finally Firefox, this is a browser developed by Mozilla foundation and hundreds of volunteers. It uses Gecko as its layout engine and the newest official version is Firefox 23.

**ADVANTAGES**

Abundant open-source and cross-platform extensions is a great feature of Firefox, with which a terrific amount of functions can be realized. To cap-

ture and download video streams, to read PDF online, to extract Flash, Mouse Gestures, Super Drag, to fulfill a form, to block an ad, etc. You name it. It can really be a powerful and efficient browser if the users use it skillfully.

**DISADVANTAGES**

Misfortune may be a blessing in disguise, and vice versa. If the rich extensions be installed randomly without choice, the browsing speed can be affected to get slow and even collapse. It also has a tardive startup and high usage of memory, which will be analyzed later. Meanwhile, its compatibility is not that good as IE's. Some webpages not strictly complied with W3C standard may not be normally displayed.

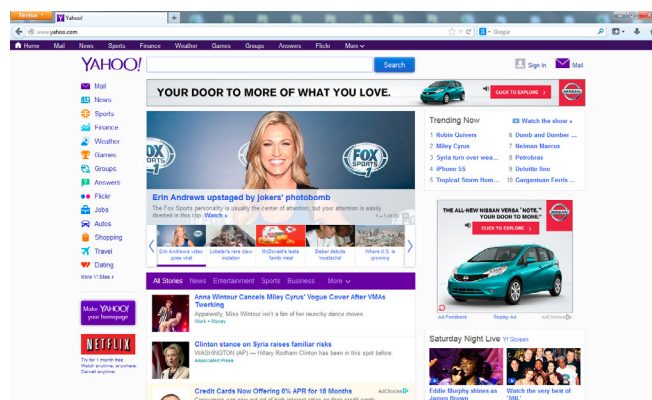


Figure 2. Destination site opened in Firefox

**CHROME**

Google Chrome, an open source webpage browser developed by Google, is written based on other open source software including WebKit and Mozilla. It aims at stability, speed and security and has created a user interface with minimalism and efficiency. The name of this software is from an internet browser GUI called Chrome.

Since its beta version released on Sept. 2, 2008 supporting 43 languages and operating systems including Windows, Mac OS X and Linux, Chrome is rapidly occupying the market, thanks to its outstanding minimalism and fast speed. A youngest browser among the 5 brands, it has already holden a position among Top 3.

**ADVANTAGES**

Succinct interface. Even the Tabs have all been minimalized to the top, leaving the most visual space to the users.

It's so fast when opening a webpage, especially impressive in dealing with Javascript.

Security. It uses sandbox technology and has been the first to offer Incognito browsing mode, which makes webpage browsing untrackable.

Finally, it uses thumbnails to display webpages viewed and often viewed. Although a small improvement, it makes more convenient for the user

to revisit the webpages and therefore a big success in advancing user experience. This feature is now widely adopted by other browsers.

## DISADVANTAGES

It's not so smooth in dealing Flash, sometimes even idles when playing flash games.

Its quantity and function of extensions cannot be compete with Firefox.

Not enough compatibility to JS. It uses self-developed V8 JavaScript Engine.

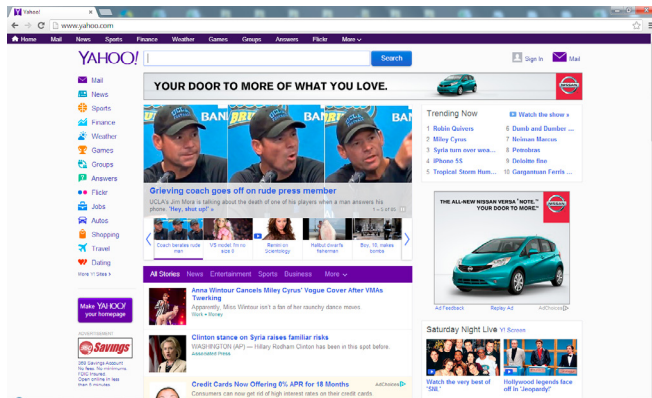


Figure 3. Destination site opened in Chrome

## SAFARI

Safari is the browser in the newest os Mac OS X of Apple computers. It uses KHTML of KDE as the operational core and uses Webkit as its layout engine like Chrome does..

First beta version released on Jan. 7, 2003, Safari has been the default browser in Mac OS X v10.3 and above and the appointed browser for iPhone and iPod touch.

The first beta version for Windows was released on June 11, 2007 and it supported Win XP and Vista. On Mar, 18, 2008, the first official version released. It has absolute advantage in mobile terminals. However, some functions like Gesture support are missing in Windows version.

## ADVANTAGES

Succinct interface, fast speed in opening webpages, low memory usage.

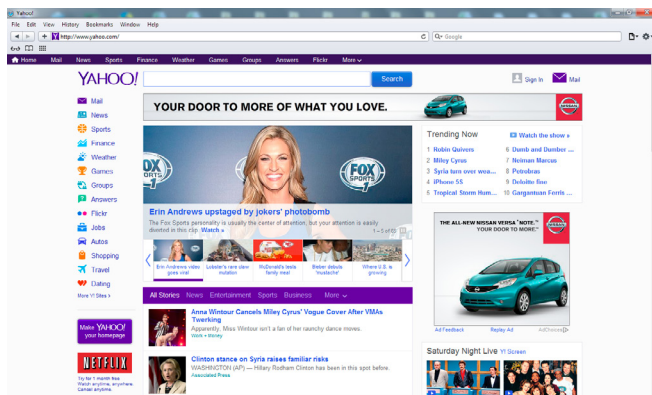


Figure 4. Destination site opened in Safari

## DISADVANTAGES

Not enough Extensions. Still less experienced in supporting Windows and therefore a lot to be perfected (Figure 4).

## OPERA

Developed by Opera Software, Opera browser is a multi-platform browser compatible with multiple platforms, operating systems and built-in internet products. It supports kinds of operating systems like Windows, Linux, Mac, FreeBSD, Solaris, BeOS, OS/2, QNX, etc. Meanwhile, it's the first browser to adopt speed dial, which has since been used by all the main-stream browsers in different formats.

Opera used Presto as its layout engine in the beginning, then changed to Webkit as Chrome and Safari did. It now uses Blink in newest version, following Google's steps, which also makes it similar enough to Chrome in browsing speed and cache dealing.

## ADVANTAGES

Succinct interface, fast speed when opening webpages especially pages with graphics, low memory occupancy, and high security.

## DISADVANTAGES

Not enough Extensions. It's sometimes annoying when the browser automatically opens all the

Table 1. Test Environment

Operating System	Windwos7 Ultimate Sp1 64bit
CPU	Intel Core i53570K
Graphics	Catalyst 12.6 WHQL, ForceWare 301.42 WHQL
RAM	4GB
Hard Disk	1T
Version of IE	10.0.0.9200
Version of Chrome	29.0.1547
Version of Firefox	23.0.1
Version of Safari	5.1.7
Version of Opera	16.0.1196

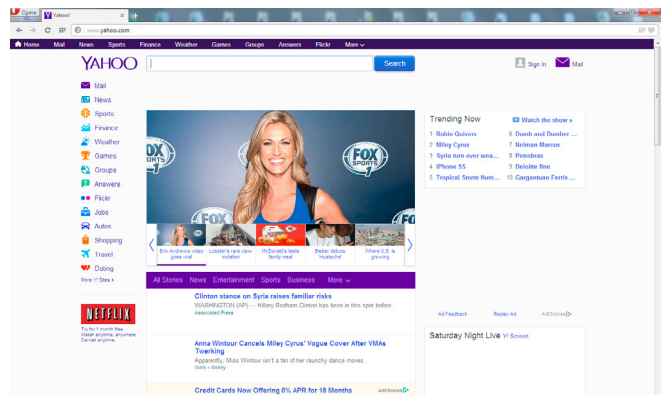


Figure 5. Destination site opened in Opera

**Table 2.** Startup Speed Comparison

Browser	Cold Start (s)	Warm Start (Avg. Of 5) (s)
IE	1.0443	0.15208
Chrome	4.4451	0.29854
FireFox	4.8830	1.06692
Safari	4.3361	0.36090
Opera	4.7414	0.30796

webpages opened last time every time you open Opera. You have to close every tab manually before turning off Opera, and therefore time is wasted (Figure 5).

**PERFORMANCE COMPARISON**

Test Environment (Table 1).

**Table 3.** Webpage Loading Speed Comparison

Browser	20KB/s	50KB/s	100KB/s	Unlimited
IE	Page started displaying after 30 seconds	Page started displaying after 7.8 seconds	Page started displaying after 5.5 seconds	Fully loaded after 5.05 seconds
Chrome	Page started displaying after 25.6 seconds	Page started displaying after 6.8 seconds	Page started displaying after 6.5 seconds	Fully loaded after 5.02 seconds
Firefox	Page started displaying after 21 seconds	Page started displaying after 9 seconds	Page started displaying after 5.5 seconds	Fully loaded after 5.80 seconds
Safari	Page started displaying after 4.5 seconds	Page started displaying after 4.3 seconds	Page started displaying after 3.4 seconds	Fully loaded after 5.12 seconds
Opera	Page started displaying after 19.5 seconds	Page started displaying after 7.4 seconds	Page started displaying after 6.3 seconds	Fully loaded after 4.37 seconds

a d v e r t i s e m e n t



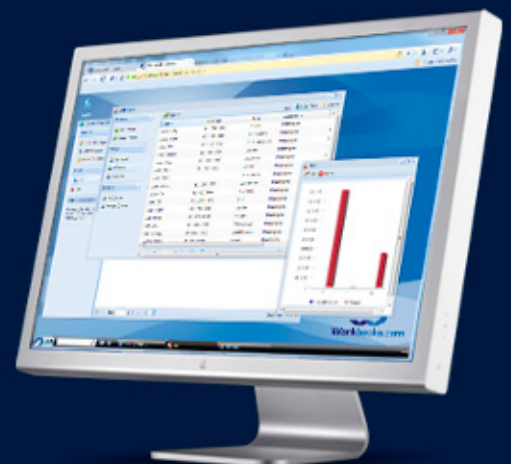
**Web Based CRM & Business Applications for small and medium sized businesses**

**Find out how Workbooks CRM can help you**

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

**Contact Us to Find Out More**

+44(0) 118 3030 100  
info@workbooks.com



## STARTUP SPEED

Here we define the Startup Speed as: The time needed from starting running the program to totally loaded with user typing acceptable. The test includes two parts: Cold Start and Warm Start. To make it ac-

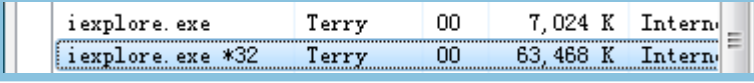
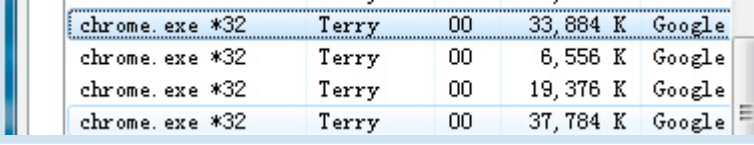
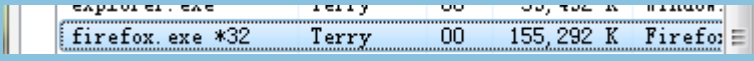

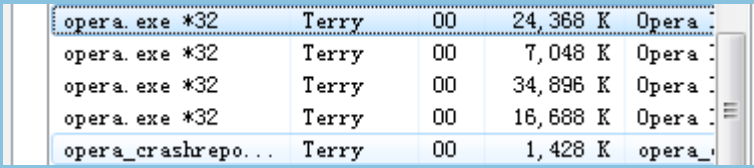
curate, we have cleared all the plug-ins to keep all the browsers not affected by any extensions.

## COLD START

The first time you run the browser after Windows starting up.

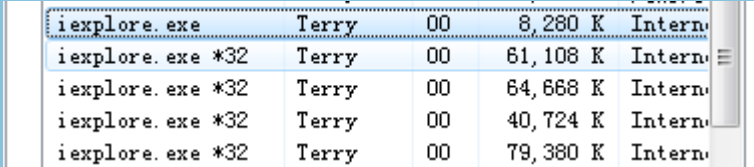
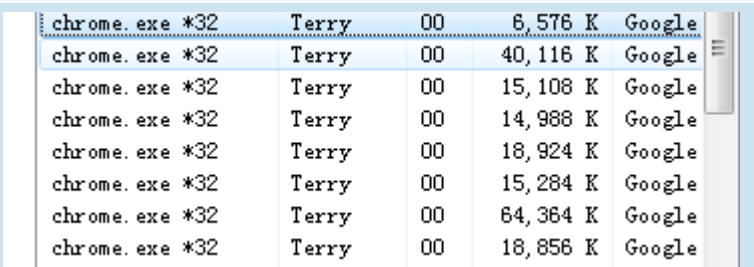

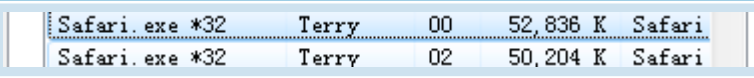
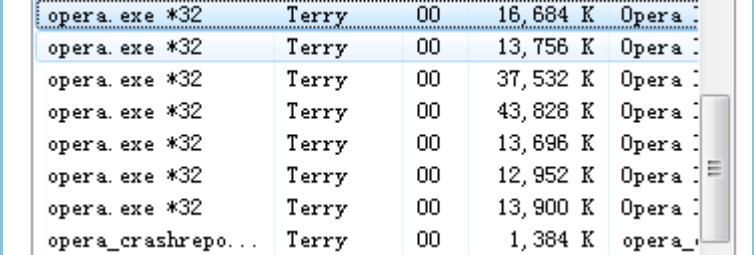
**Table 4.** Memory Usage Comparison in 1-Window Browsing;

**Figure 6-10.** Screenshots of Memory Usage Comparison in 1-Window Browsing

Browser	Screenshot	Memory Used
IE		68.84MB
Chrome		95.31MB
Firefox		151.65MB
Safari		19.98MB
Opera		82.45MB

**Table 5.** Memory Usage Comparison – 5-Window Browsing;

**Figure 11-15.** Screenshots of Memory Usage Comparison in 5-Window Browsing

Browser	Screenshot	Memory Used
IE		248.2MB
Chrome		189.66MB
Firefox		171MB
Safari		100.63MB
Opera		150.13MB

## WARM STARTS

Subsequent runs after Cold Start (Table 2).

It's easy to see that Warm Startup speed was enhanced by a large margin from Cold startup speed for all browsers. IE11 was absolutely the winner in this benchmark and the main reason was that most components needed for IE had already been loaded by os when Windows started. Chrome, Safari and Opera made a Roland for an Oliver and Firefox came last.

## WEBPAGE LOADING SPEED

To accurately compare the speed of loading the same webpage in different bandwidth environments, we simulated low-speed bandwidth conditions and limited downloading speed respectively to 10KB/second, 20 KB/s, 50 KB/s, 100 KB/s and unlimited. We also cleared all the browsing caches to guarantee the accuracy of the test. We used Yahoo.com as the destination site for this test (Table 3).

## MEMORY USAGE

When opening only one browsing window: Table 4.

Least memory used, Safari had an absolute advantage here when opening only 1 browsing window. IE, Opera and Chrome were close because they adopt the dame core, and Firefox came last.

When opening 5 browsing windows at the same time: Table 5.

Seen from the table above, Safari won again by a large margin. IE had some advantage in only one window condition, but it used the most memory in multi-window condition. The figures did not change much under the two conditions for Firefox, therefore, it has more advantages when more windows are opened. Chrome and Opera gave mediocre performance here.

## SECURITY

Table 6. Security Comparison

Browser	InPrivate/Incognito Browse	Malware blocking rate
IE	Supported	99.96%
Chrome	Supported	83.16%
Firefox	Supported	9.92%
Safari	Supported	10.15%
Opera	Supported (Extension needed)	1.87%

The statistics are from the test report released by NSS lab.

Read More: <https://nsslabs.com/news/press-releases/which-web-browser-offers-best-malware-protection-nss-labs-releases-new-2013-web>.

Chrome exceeded IE9 in last year's test, but it

seems that IE10 has made a great improvement in security, which has made itself a winner this year.

## COMPATIBILITY

It's generally acknowledged that IE has the best compatibility and that most websites make adjustment according to IE browser' display. Firefox also does well here. Chrome used to have frequent problems with compatibility; but as Chrome is growing fast, more and more websites start to take Chrome into account when they deal with compatibility. Now most compatibility problems of Chrome have already been fixed. Safari has poor compatibility in Windows and Opera also performs mediocre here.

## EXTENSIONS

Undoubtedly, Firefox dominates this field with the powerful support of open source community.

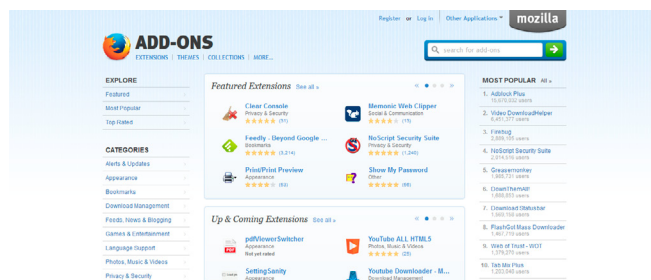


Figure 16. Extensions page of Firefox

IE has small amount of extensions, most of which are developed by Microsoft and other software companies. Its ActiveX is often exploited by malware and this is also the cause for most IE problems like collapse and tardiness.

The amount of extensions in Chrome is increasing and the functions are being expanded.

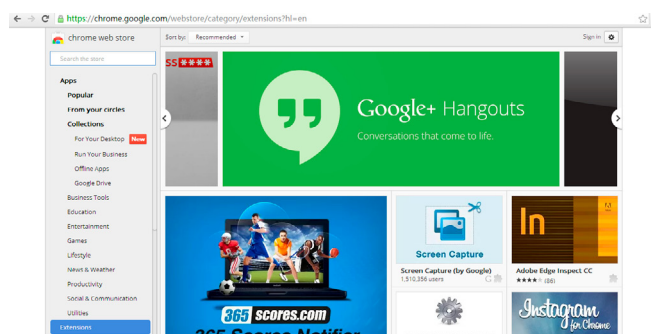


Figure 17. Extensions page of Chrome

Safari's Extensions for Windows are still conservative (Figure 18). Extensions in Opera are normally released by community and normally with high quality (Figure 19).

## SUMMARY

As an old brand, IE has the best compatibility and has made impressive improvements since IE8. We can see that MS is keeping improving IE and is guarding its place in this field.

Chrome does have advantages in speed and security. Firefox makes itself outstanding with rich Extensions and nice compatibility. Opera is kinda growing into another Chrome. Though not long enough since transplanted to Windows, Safari has obvious advantages in memory usage and web-page loading speed, according to the test above.

Each of the 5 browsers has its own outstanding features. Users can now choose freely according to own needs and habits.

## GLOSSARY

Terms Mentioned in the Article.

### TRIDENT (MSHTML)

Trident (also known as MSHTML) is the name of the layout engine for the Microsoft Windows version of Internet Explorer.

### GECKO

Gecko is a free and open source layout engine used in many applications developed by Mozilla Foundation and the Mozilla Corporation (notably the Firefox web browser), as well as in many other open source software projects.

### WEBKIT

WebKit is a layout engine software component designed to allow web browsers to render web pages. It powers Google's Chrome web browser versions up to 27, and Apple's Safari web browser applications.

### PRESTO

Presto was the purpose-built layout engine of the Opera web browser for a decade. It was released

on 28 January 2003 in Opera 7, for Windows, after several public betas and technical previews.

### BLINK

Blink is a web browser engine developed by Google and Opera Software ASA as part of the Chromium project, first announced in April 2013.

### V8 JAVASCRIPT ENGINE

The V8 JavaScript Engine is an open source JavaScript engine developed by Google for the Google Chrome web browser. It has since seen use in many other projects. As of 2012, the head programmer is Lars Bak. The first version of the V8 engine was released at the same time as the first version of Chrome, September 2, 2008.

### KDE (KOOL DESKTOP ENVIRONMENT)

KDE is an international free software community producing an integrated set of cross-platform applications designed to run on Linux, FreeBSD, Solaris, Microsoft Windows, and OS X systems. It is known for its Plasma Desktop, a desktop environment provided as the default working environment on many Linux distributions, such as Kubuntu and openSUSE.

### KHTML

KHTML is a HTML layout engine developed by the KDE project. It is the engine used by the Konqueror web browser. A forked version of KHTML called WebKit is used by several web browsers, among them Safari. Distributed under the terms of the GNU Lesser General Public License, KHTML is free software.

### GPU

A graphics processing unit (GPU), also occasionally called visual processing unit (VPU), is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display.

(Excerpts from Wikipedia.org by original user.)

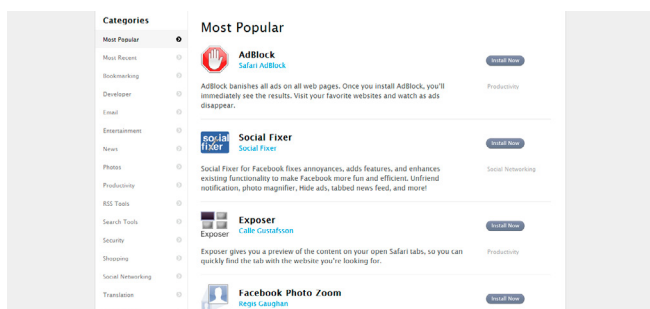


Figure 18. Extensions page of Safari

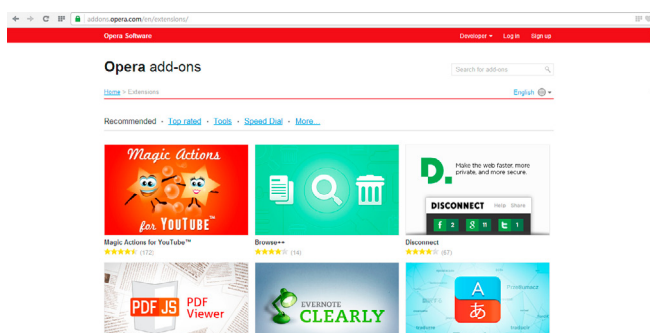


Figure 19. Extensions page of Opera

## ABOUT THE AUTHOR



Terry Tang, founder of *WiseCleaner.com* and a programmer with rich development experience, has developed *Wise Care 365*, *Wise Registry Cleaner*, *Wise Disk Cleaner* and many other popular PC utilities software.



The **only** existing System of its kind,  
IncMan Suite has already been adopted  
by a host of corporate clients worldwide

## The Ultimate Forensic Case Management Software

Fully automated Encase Integration

Evidence tracking and Chain of Custody

Supports over 50 Forensic Software and third parties

Training and Certification available

Special discount for LEO, GOV and EDU customers



**SPECIAL PROMO 15% OFF**

single user perpetual license

<http://www.dimmodule.com>

promo code **E-FORNCS13**

DFLabs DIM is a forensic case management software that coherently manages cases, data input and modifications carried out by the different operators during Digital Evidence Tracking and Forensics Investigations.

It is part of the IncMan Suite, thus it is able to support the entire Computer Forensics and Incident Response workflow and compliant with the ISO 27037 Standard.

[www.digitalinvestigationmanager.com](http://www.digitalinvestigationmanager.com)

# CLOUD



by Rick Clark

Cloud collections, cloud storage, collections through the cloud, cloud, cloud....cloud. Cloud is such a simple term, but has many meanings, implications and applications to the forensic and legal industry. I believe the growing confusion in the legal space is due to the need to categorize the applications of cloud offerings and how to best utilize them.

#### What you will learn:

- What cloud really means for the forensic and legal world
- Three popular categories of “legal” cloud – Storage, Collection and Data Review
- Specific technologies and workflows that fit in these categories
- Questions to ask software and cloud providers to ensure you are covering all bases

#### What you should know:

- Basic e-discovery knowledge and the litigation process
- Forensic processes and workflows with data collection
- Familiarity with the Electronic Discovery Reference Model

I recently attended the Masters Conference in Washington DC and saw a very smart panel discuss how the legal industry is approaching eDiscovery data management and that applies to cloud services. Initially, my thought was that it was a panel on Cloud Collections (as mentioned in the title) and data review, but much to my chagrin it was simply on the basics of cloud storage for the law firm market. When the discussion on cloud collection came up, it was barely covered and seemed like it was not something that can be handled well and with much caution. This affirmed more how important this topic is for the forensic and legal world. In this article, I will discuss the three main use market use cases for “cloud management” (I’ll call it for now) for the forensic and legal industry.

#### THE THREE LEGAL CLOUD CATEGORIES

Before I dive right in to the Cloud discussion, I think it is worth mentioning that my interpretation of Cloud is simply a “new definition of the Internet as it pertains to hardware access.” NOT to simplify it even further, but in many cases, that is all it is. Where does the information physically reside and how does that affect my bottom line? It is just what one does with this rapidly changing technology and space, that is important.

The first and most discussed in the legal industry is Cloud Storage utilized by corporations and law firms. Likely, everyone reading this is aware of the sizable and growing storage necessity for corporations to retain data in the event it is necessary for litigation or other purposes. IT infrastructures, Software License fees, Human costs



all contribute for companies to look at other options to shave off rapidly growing costs associated with data storage and management. As stated by the National Institute of Standards and Technology (NIST) Cloud is defined as, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."<sup>(1)</sup> I oversimplified it, they really defined it. But the point is that there is a large need; it is available, accessible and needed.

Leveraging silo's that are created to act as a third party storage and data management are very appealing. Sadly, many are realizing that they aren't created with the litigation hold to discovery process and so many concerns need to be taken into consideration:

- Are they secure to handle extremely sensitive data?
- Are they going to be in business for the long-term?
- Is the data easy to access for collection and discovery purposes?
- Are the servers based in the US, or are they subject EU or other privacy laws?

What does the End User License Agreement state on privacy, security, data ownership etc? There are many more and generally specific to the corporate practices of individual companies.

The second usage for the cloud that affects corporate policies is Personal Cloud use. This will include Dropbox, LinkedIn, Facebook etc. There are many discussions around the perils of Bring Your Own Device (BYOD) if the policies aren't strictly enforced, and utilizing these cloud based technologies is not much different. The policies surround protection of data, data security and preparation for future collections (among many other policies). At the moment, BYOD is not a generally recommended idea, but widely used among corporations and law firms because policies are still getting developed. If your firm does not have policies, it is very important to start that process of learning best approaches to reel in to a standard practice. All of that mentioned, for BYOD, utilizing facebook, personal emails etc. they are all discoverable and the way in which it is getting discovered is all over the map and just getting figured out. For example, there have been a few cases recently where access to information on Facebook was used to demonstrate a difference in actual conduct compared to the disability claimed (*Loporcaro v.*

*City of New York*)<sup>(2)</sup>. A good quick synopsis of this case and others can be found on X1's website <sup>(3)</sup>. The easy take-away here is that whether you are sending emails that could indict you or posting it on your personal Facebook page, all are potentially discoverable (So if somehow this is slapping you in the face...just know that everything that is recorded, voice or text, could be discovered, so always proceed with caution).

As a general rule, no corporation can control the usage of personal accounts no matter what the policy as long as it isn't transferring company information. The typical use case where an employee can send documents both personal and company would be with DropBox, and is used often. Personal email, like Gmail, is another where both company information and personal information could reside and be considered for evidence.

The third usage for cloud would be focused on the e-discovery arena where individual accounts are part of the e-discovery process and need collecting. Assuming that custodians are using any and all of their social media, personal media and company for personal and company information, it is discoverable and would need to be harvested forensically and reviewed. Initially, this process was difficult and burdensome. Fortunately, technology exists to ensure the forensically sound process of collecting the email, social media etc. and any live unstructured data. To be clear, as I move through this article, normal means of on-site forensic acquisition is always an option, but the purposes of cloud collections will be for remote collections.

## EVOLUTION OF E-DISCOVERY SOFTWARE

In a previous article, I discussed the evolution of e-Discovery software. It is important to understand that information as we discuss the workflows for cloud collection, which is the crux of my focus for this article. Please feel free to skip this section if you have already read this or have a good understanding. In May, 2005 George Socha and Tom Gelbmann put together the Electronic Discovery Reference Model<sup>(4)</sup> to help create a standard or guideline for the legal industry to follow when offering services or creating software to address the growing demand to manage data for discovery in litigation (Figure 1).

Initially, most software utilized to collect, cull and review data was repurposed from other market sectors. For example the main collection tools used to forensically mirror hard-drives were EnCase from Guidance Software and the Forensic Toolkit from Access Data. Both create an exact mirror image of a hard-drive that includes deleted and live files to preserve all metadata and data files just as its original. This technology was heavily used worldwide typically in police departments and state agencies to examine hard-drives

from suspects. Their immediate need in the legal space made them the fastest growing collection tools and a standard practice for getting the data ready for attorney review. Once the data was collected, the initial process was to convert everything to a TIFF to review in Summation (now owned by Access Data) or Concordance (now owned by Lexis-Nexis) as they didn't initially allow for near native file review. To convert to TIFF images with load files teams would process the collected data in LAW (now owned by Lexis-Nexis) or IPRO. This workflow was well established because of paper discovery where they would scan and convert to a TIFF. Since TIFF was the standard format, all workflows were built around it for paper and Electronically Stored Information. The major issue the industry was facing was the high expense to converting to TIFF for review and many cases were forced to settle early without discovery.

Knowing TIFF conversion and review was a huge hinderance to the litigation lifecycle, native processing and review solutions hit the market. Wave Software had Trident Pro where all unstructured data was pre-culled before a process in LAW or IPRO. The culling process included removing the system files utilizing the NIST database of MD5 hash codes for the common system files, Boolean Key Word Filtering and exact-hash duplicate removal utilizing a SHA-256 has of key components of the email message within a PST or NSF or files. Nuix is another native processing application that similarly culls down data to make the data more manageable for discovery. Nuix,

though, takes the workflow an extra step to have a first pass review to eliminate obvious non-relevant data (typically Spam, personal messages, newsletters etc.) then only publish to the attorney review the mostly relevant.

As review platforms became more accustomed to rendering data in its native format, more cases were able to be hosted without any conversion. One of the first to do this well was iCONNECT with its nXT product where it would take a load file created from any native processing solution and render the file as if it was in the format it was originally viewed. Not long after, Kcura created Relativity and continued to normalize a native processing to native review/production workflow. Both nXT/XERA (iCONNECT's latest release) and Relativity allow for a production to TIFF or PDF from the review application of ONLY what is relevant for the production.

This brings us to where we sit today as the next generation with a suite of offerings that allow forensic departments and companies to provide a full offering from collection to investigation to review and production. Many e-discovery providers are in the middle of the EDRM and working left toward collection and many forensic teams are at the beginning and working right toward processing, analysis and review.

### CLOUD COLLECTION

There are many ways to approach a collection, but few take into consideration the cost sensitivities, speed and workflows needed for the legal and investigation industries and approach it as a whole.

## Electronic Discovery Reference Model

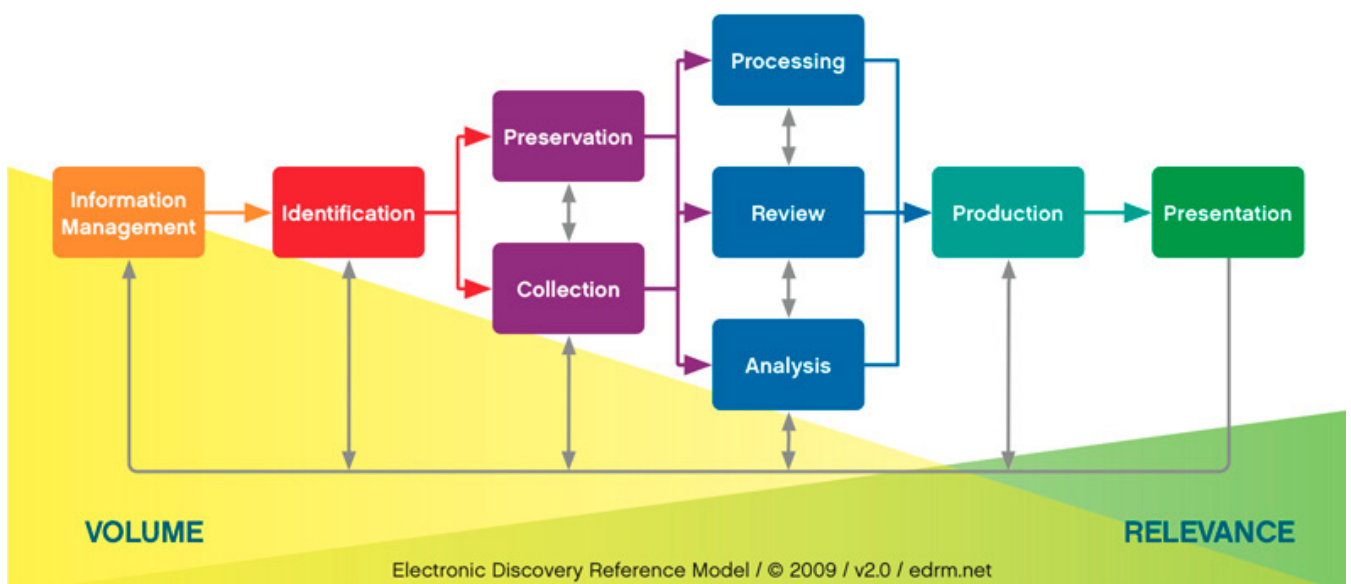


Figure 1. [www.edrm.net](http://www.edrm.net)

I will explain what I mean by “few” by highlighting some examples of software that create an easy workflow from Litigation Hold to first pass review with social media sites and cloud based email. Primarily, I will be discussing two platforms that do a great job at capturing data in a forensically sound manner for Gmail, Hotmail, Facebook, Dropbox etc.

The significance of this technology isn't totally in the process, features and ease of use, but the business aspect it brings to the community.

One of the biggest challenges in the legal industry or the costs of eDiscovery. I could write a piece just on that, but there are some really good articles on the subject that describe the costs and how generally they outweigh the outcome of the case. Most cases settle because of costs than the merits of the case, sadly.

The key costs involved in eDiscovery are:

- Per GB processing, analytics and hosting fees
- Linear Attorney review – billable hours and is the highest cost
- Over collection of data – causes an inflated downstream cost with the first two points

## E-CLOUDCOLLECT – CLOUD COLLECTION SOFTWARE

Technology companies may seem like they spring up from anywhere and everywhere, but when you research the roots as part of your general due diligence, you may find that “why” they developed the technology is a main reason to do business with them. eCloudCollect was born out of the legal eDiscovery industry and is focused on its clients and prospects to level out many unneeded costs in “cloud collection forensics”. Being built to address second cloud category above, they have created a seamless workflow that allows a law firm, corporation or forensic service provider to harvest ESI that is in Gmail, Hotmail or other web email applications quickly and easily.

Once a litigation hold is in place the IT group may issues alerts to the individual custodians that have ESI in the cloud or even their local workstation. The alert gives the custodian the option to input their credentials and allow the system to login to Gmail, Hotmail etc. and pull their data into an XML format for further review. The process is not only fast, it is simply running in the background as to not interrupt the custodian’s environment.

“eCloudCollect is designed to perform targeted collections of online and remote data without business interruption and now offers the option to upload and preserve collections in the cloud or download onto an encrypted physical device which addresses size, bandwidth and time constraints that other remote collection tools face and eliminates the need for on-site travel when performing targeted collections,” said Sarah Thomp-

son, Cumulus Data’s Vice President of Product Management. “By taking advantage of the economies of scale that cloud computing provides, we can offer truly disruptive pricing. We believe this is a game changer and are excited to bring it to market.”

Sarah sums it up best with what the company can do overall, but the software begins to speak for itself with an easy interface and “get to the point” workflow.

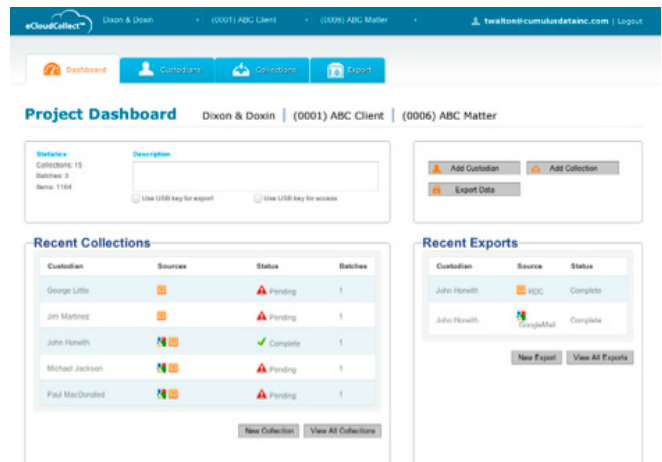


Figure 2. Project Dashboard – demonstrates the overall look at the projects

Many Certified Computer Examiners are used to a tedious collection process to address slack space and regeneration of deleted items, but with the adaptations of better retention policies and easier exports from archival systems the need for high level forensic acquisitions is shrinking. A major decline lies in the fact that case law now supports high sanctions for intentional spoliation, which deters even small companies from deleting important items.

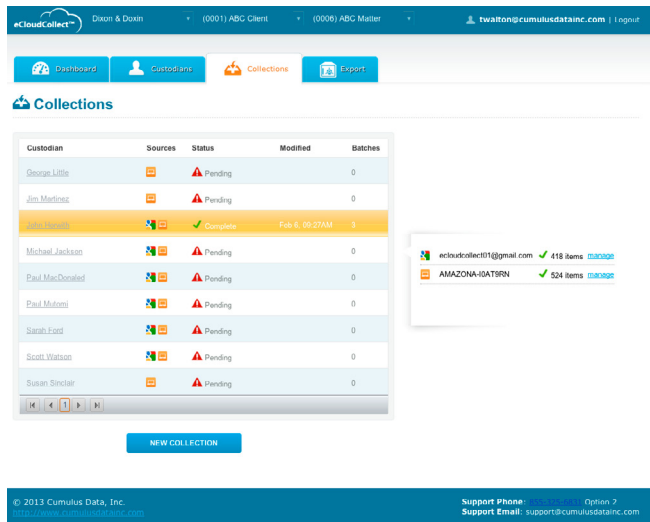


Figure 3. eCloud Collect

When setting up new projects or a collection, the interface allows users to easily path to the data over the internet with a secure connection.

Demonstrates the different sources eCloudCollect harvests data.

No matter where the user is, there is a secure workflow to collect email, laptops, servers, desktops, as a remote collection.



**Figure 4.** Easy Navigation to start new collections

## SECURITY CONSIDERATIONS FOR E-CLOUDCOLLECT

The eCloudCollect platform is a controlled and secured environment that adheres to security standards with credentials that include; SOC 1/SSAE

### ON THE WEB

#### Legal Research Links

- [www.edrm.net](http://www.edrm.net) history of e-discovery, resources and articles
- [www.law.com](http://www.law.com) articles and new trends in e-discovery
- [www.sochaconsulting.com](http://www.sochaconsulting.com) Information on service providers and legal technology

#### Technology Companies

- [www.nuix.com](http://www.nuix.com) mentioned in this article for preprocessing
- [www.iconect.com](http://www.iconect.com) mentioned in this article for review, analysis and production
- [www.discoverthewave.com](http://www.discoverthewave.com) mentioned in this article for native data processing
- [www.guidancesoftware.com](http://www.guidancesoftware.com) mentioned in this article for data collection
- [www.accessdata.com](http://www.accessdata.com) mentioned in this article for data collection and Summation
- [www.lexisnexis.com](http://www.lexisnexis.com) mentioned in this article for Concordance review platform
- [www.kcura.com](http://www.kcura.com) creators of Relativity which is a legal review platform
- [www.ipro.com](http://www.ipro.com) mentioned as a data processing company
- [www.cumulusdatainc.com](http://www.cumulusdatainc.com) featured in this article for cloud collection
- [www.cloudpreservation.nextpoint.com/](http://www.cloudpreservation.nextpoint.com/) featured in this article for social media and website collection

### REFERENCES

- <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Loporcaro v. City of New York and Perfetto Contracting Company, 35 Misc.3d 1209(A), (N.Y. Sup. Ct. Apr. 9, 2012)
- <http://blog.x1discovery.com/2012/05/08/social-media-case-law-update-volume-of-cases-accelerating/>
- [www.edrm.net](http://www.edrm.net)

16/ISAE 3402, FISMA, Moderate PCI DSS Level 1, ISO 27001, International Traffic In Arms Compliance and FIPS 140-2. In addition to built-in user level security, all files are hashed during collection, re-hashed after upload and preserved into a 256-bit encrypted vault ready for review and workflow exporting. eCloudCollect employs a two-factor authentication process to export data.

## FACEBOOK AND SOCIAL MEDIA COLLECTIONS

As stated above, there is a growing need to acquire information from a users Facebook, Twitter or other social media sites as it pertains to the case. It could be because it is confirming or contradicting the alibi, confirming connections to individuals or simply demonstrating the individual is able to work, stand or swing an ax. Regardless of the need, it is becoming a growing evidence haven for many small cases. This is important to the point made on the costs of eDiscovery as many defendants and plaintiffs can't afford the general high costs of litigation, but the evidence is crucial for the guilt or innocence of the individual or company.

Nextpoint is a company that has created a tool-set that include cost efficient collections of social media and websites. Also created from a group of individuals from the legal industry, Nextpoint has created a workflow that has Litigation Hold, Preservation to Review and Production in mind. All steps have easy audit trails and all metadata is secured. The importance of this information is always varied, but the ease of access and cost structure allows for discovery better strategies to get created and deployed.

## SUMMARY OF TECHNOLOGY HIGHLIGHTS

No matter how you look at the various technologies, it is important to proactively search and stay up on what new platforms are being created. The landscape will always change as we continue to grapple with types of law suits that surround personally used social media, data repositories or devices. The technology likely exists to solve the problem. If it impacts your business, it should be a priority to stay on top of the latest technological advances.

## ABOUT THE AUTHOR

*Rick Clark has been in the legal industry since the early 2000's starting as a discovery consultant. He was a co-founder of Wave Software and The Masters Conference for legal professionals. For the past seven years he has worked with many corporations, government agencies, law firms, consulting companies and legal service providers as a technology consultant. In his spare time he likes to cook, write, garden, paint and hike and currently resides in Herndon, VA with his wife Amy. [http://www.cozen.com/Templates/media/files/Dropbox\\_and\\_the%20Impact%20of%20Personal%20Cloud%20Storage.pdf](http://www.cozen.com/Templates/media/files/Dropbox_and_the%20Impact%20of%20Personal%20Cloud%20Storage.pdf).*



ELEVENTH ANNUAL  
HITB SECURITY  
CONFERENCE  
IN ASIA

**REGISTER ONLINE**

<http://conference.hitb.org/hitbsecconf2013kul/>

# HITBSECCONF2013 KUALALUMPUR

October 14th - 17th 2013 @ InterContinental Kuala Lumpur

## 8 NEW TRAINING COURSES (14th - 15th October)

- Extreme Web Hacking
- Windows Kernel Internals
- Blackbelt Penetration Testing
- The Art of Exploiting Injection Flaws
- The Android Exploit Lab
- Advanced iOS Exploitation
- Introduction to iOS Exploitation
- Building Secure Web & Mobile Applications

## CONFERENCE KEYNOTE SPEAKERS (16th - 17th October)



**ANDY ELLIS** (Chief Security Officer, Akamai)



**JOE SULLIVAN** (Chief Security Officer, Facebook)

# GOOGLE CHROME – THE FUTURE OF WEB COMPUTING

by John Blossom

By many estimates the browser wars are over, and Google Chrome has won. Yet although Google Chrome has become a broadly used tool for accessing and publishing Web information, the full impact of Chrome is just beginning to come into focus for many people. What is Chrome all about, and where is it taking us? John Blossom, President of Shore Communications, Inc., is a leading content and technology industry analyst who sees the evolution of Google Chrome as a major factor in the development of secure, Web-centered computing services.

## What you will learn:

- How Google Chrome came into being and its principle design features
- How Google Chrome security differs from other major Web browsers
- How Google Chrome is expanding the capabilities of platform-independent computing
- The meaning and value of an expanding range of devices based on Google's Chrome OS operating system

## What you should know:

- Google Chrome is more than just a browser – it's in effect a secure Web-based operating system that can run on any common personal computer or mobile device. As such, Google Chrome challenges us to think about how Internet-based "cloud" computing resources can enhance the information experience through sophisticated, secure and platform-independent computing.

In September of 2012, something happened that was not noticed very widely, but which had major significance for the future of computing on the Web. It was then that the Web monitoring service StatCounter recorded for the first time in its data gathering that Google's Chrome browser had become the most used Web browser on desktop and laptop computers. Chrome had finally eked out a small lead over Microsoft's Internet Explorer browser, and was being used significantly more than its other major browser competitors – the Firefox browser from the Mozilla Foundation and Apple's Safari browser.

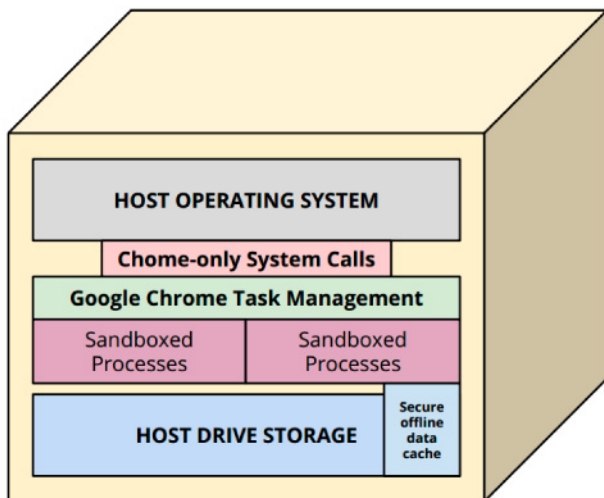
A year later, Google Chrome is now clearly the dominant desktop and laptop browser used on the Web today. According to StatCounter, Chrome is used by about

43 percent of Web users on their computers, whereas Internet Explorer is used by about 26 percent of Web users on their computers and Firefox by about 19 percent. Since StatCounter's statistics are based on a sample of Web users their data is but one way to measure the so-called "browser wars" between technology giants. However, as widely referenced data, it's a good yardstick for considering just how quickly Chrome is growing and to consider seriously the implications of its growth.

It's important to consider Chrome very seriously for any number of reasons, but I believe that the primary reason to focus on Chrome is that Chrome represents something bold and ambitious in the realm of computing. To me, Chrome represents the first true high-performance,

secure cross-platform computing environment that is being adopted on a global basis. In essence, Chrome has become its own operating system – regardless of the computer on which it operates – that encapsulates the data that it manages in a way that makes much of the computer that supports a Chrome browser largely redundant or obsolete for performing many high-value tasks on a computer.

In the process of becoming more like a general-purpose computer within a computer, Google Chrome is encouraging a new generation of applications software to rise to prominence, not as “good enough” substitutes for desktop computing resources but as “best of breed” solutions that challenge us to consider just how powerful Web computing has become and how much power that it has yet to unleash.



**Figure 1.** *Google Chrome – General System Architecture*

## ORIGINS OF GOOGLE CHROME

Google Chrome launched in September of 2008 for public use as a free beta version browser available for users of Microsoft Windows PCs. At the same time Google released a great deal of Chrome’s code via the Chromium open source project. This dual-track provision of both open source code and Google’s own version of that software has become a familiar product development strategy for Google. We see the same methods at work in Google’s Android operating system, which has both open source and privately maintained components, as well on many of its toolkits and platforms today. This has allowed Chrome development to proceed rapidly both with the support of a large open source software development community and with Google’s own programming teams more focused on its down design and strategy goals.

Let’s recall that when Google Chrome first launched, the browser wars were in a much different place than they are today. Microsoft PCs were

by far the dominant computing platform for accessing the Web, with Microsoft’s own Internet Explorer browsers serving about 67 percent of Web browser use. The presence of Google Chrome was for several years just a rounding error in the larger battle between Internet Explorer, Firefox and Safari, just as Google’s Android operating system was largely discounted as a factor in the mobile device marketplace. Yet now we see both operating systems being dominant on a global basis. A lot has changed in just a few years – and the design and strategy behind Google Chrome are a key factor in those changes.

## KEY CHROME DESIGN PRINCIPLES

When Google Chrome first launched, it was a collection of features both relatively old and relatively new. The old parts of Chrome centered on the widely accepted World Wide Web Consortium (W3C) standards for browser-based computing centered on the Hyper-Text Markup Language (HTML). Chrome adhered to HTML standards pretty much the same way that any other browser did, and supported common programming and media management services such as JavaScript and Adobe’s Flash media player. But there were a few key design considerations that set Chrome apart from other Web browsers pretty distinctly. A newer component that was available for Chrome development initially was WebKit, a cross-platform software toolkit for Web browser development that had been turned over to open source development by Apple in 2006. Until fairly recently, most Web browsers have used WebKit components to process Web content in browsers.

The first key difference for Chrome was that each browser window or tab that was open at a given point ran as a computing “process” that the main Chrome browser program launched. At the time this was very unlike other Web browsers, which typically had either one full instance of its program launched for each browser window opened, or it managed all of its browser tabs within a single instance of its program. In other words, Chrome was the first browser to manage specific displays of information in Chrome as sub-programs all of their own. Chrome was acting more like the computer operating systems on which it ran than was acting like just another program on that computer. This allowed for much more stable operation: if, for example, one Web page or program in a given Chrome tab crashed, that crash was far less likely to affect other process operating under Chrome.

The other key factor that was introduced in Chrome browsers was the notion of “sandboxing” the processes providing users with Web services. In other browser designs it had been common for one browser window or tab to be able to communicate with another window or tab fairly openly,

as well as with the underlying computer. While Chrome accommodated these sorts of communications, it introduced the concept of encapsulating the processes providing services in Chrome windows and tabs in their own data spaces, with carefully restricted access to both other browser windows and the underlying PC. Eventually Chrome would add “Safe Browsing” features as well – essentially malware detection software and services operating mostly via Google’s own Web servers.

Within Chrome’s own sandboxed computing resources, there was no foothold for malware to lodge itself, as its design and insulation from less secure computing resources left little for exploit programmers to attack. Microsoft has adopted some of the principles of sandboxing to its Internet Explorer browser, but since its browser plugins often access PC-based data and software, there are limits to its effectiveness. Recently Google announced that in a year’s time it will be eliminating Chrome support for such platform-specific plugins, further enhancing the security of its sandboxed processing.



**Figure 2.** *Demonstration of 3-D Motion-Activated Game via Google Chrome*

## CHROME VERSUS COMPETITIVE BROWSERS

The combination of separate processes, sandboxing and malware detection introduced a combination of performance and security features that set Chrome apart distinctly from other browsers available at the time. In more recent years many other browsers have adopted these sorts of features, but so far none have combined them to the extent that Google Chrome has to provide a secure, cross-platform computing environment. Though these other browsers have improved significantly, there are conflicts of interest that prevent them from performing at quite the same level as Chrome in many instances.

In the instance of Internet Explorer, Microsoft continues to try to integrate components into its browsers that provide software and access that

integrates its browsers into the underlying computing environment more directly. Apple’s Safari browser does this also, though to a lesser degree. In other words, in order for these computer makers to keep their non-Web software and services from becoming irrelevant to Web-centric computer users, they are more likely to make their browsers extensions of their computers than extensions of the Web computing environment. This opens up inherent exposures to security flaws in these browsers, flaws which have been exploited regularly via computer malware. Chrome may support some of these exploits also when a user gives a file or program access to their computer, but primarily the design of Chrome itself does not support these exploits.

Firefox does not have the same sort of issues with attachment to underlying computers, but as a nonprofit organization it does have the problem of needing revenues from marketing alliances with Web sites operated by media companies that want to use Firefox to promote ads and services via site-specific “toolbars” inserted into the top pane of a browser display. These toolbars tend to affect overall browser performance and introduce a level of “eavesdropping” on a user’s Web activity that introduces security concerns of their own. By contrast, browser “extensions” allowed in Google Chrome browsers are processes that work in the same sort of sandboxed fashion as do processes operating browser tabs, providing more secure and contained value-add functionality.

In short, Chrome exists neither to promote hardware nor specific media sources: it exists to promote the Web, from which Google derives meaningful data – “signal” that drives its revenues from online ads across the Web and its own services. It could be argued therefore that Chrome exists for Google to beat its competition at getting better signal for its ads, but as we’ll see there is a broader strategy in play that goes far beyond ads. The broader underlying strategy is to maximize open Web signals available for everyone to interpret for products and services. When the Web wins, Google wins – and they would like us to think that the opposite case applies often, as well. Given Google’s broad commitment to open source software on the Web, it’s a compelling argument for many people.

The Google Chrome and Chromium software continues to develop rapidly, pushing releases out on a very regular basis. Major releases come out every four to six weeks, typically, and minor bug fixes may come out as often as once or twice a week. These are loaded automatically every time the browser is restarted, or may be reloaded manually via an icon that appears in the Chrome browser when an update is available. Typically a manual restart for updates will leave a user’s browser in the same state



that it had been before the application of the update, generally only a few seconds later.

So the Google Chrome experience on desktop and laptop PCs is largely transparent to the users as a software experience – the software appears to be “just there” almost all of the time. This stable, secure, hassle-free Web computing environment has been the core of Chrome’s appeal to typical Web users, who are eager to have uninterrupted, high-performance access to the Web. For those people who want to experience the “latest and greatest” versions of Chrome before their release as production-grade features, Chrome can be configured to accept “Developers” and “Beta” versions of a new release, enabling Google to get valuable feedback from users that like to try out new and potentially unstable software features and services.

### CHROME FOR MOBILE: EXTENDING INTO NEW PLATFORMS

Recently Google Chrome design has broadened significantly, both in the breadth of the platforms that it supports and in the features that it provides for Web-centric computing. From its start as a secure and stable browser on Windows PCs Chrome has expanded to provide services on a very wide variety of computers. Chrome is available on desktop and laptop computers for Microsoft Windows, Apple’s Mac OS X and computers using variants of the open source Linux operating system. As mobile phones and tablets have become much more pervasive tools for accessing Web content, Chrome has extended its reach on to many of these devices also. There are Google Chrome browsers available for devices running Google’s own Android operating system as well as for Apple’s iOS mobile operating system for the iPhone and iPad line of devices. Through its Chromium open source versions, Chrome is also adaptable to virtually any other computing device available today.

While mobile versions of the Chrome browser work similarly to desktop/laptop versions of Chrome, their functions are not exactly the same. For example, mobile versions of Chrome do not support all forms of media display or the browser extensions supported by PC-based versions of Chrome, due to performance considerations and licensing issues specific to many mobile devices. Also, to accommodate the touchscreen-centered access to Web content that today’s mobile devices support, the interface design of mobile Chrome browsers is significantly different from its PC versions. However, increasingly the software used in Chrome browsers for mobile devices is a close equivalent to the software used in its desktop/laptop PC versions, with a strong overlap of performance and security features.

The merging of Chrome versions for PCs and mobile devices is accentuated in part because Google sees the importance of ensuring open Web content and services in a mobile world. The importance of Chrome for mobile devices as a key component in Google’s strategies was emphasized when Google appointed Sundar Pichai as the head of both Android and Chrome development in May 2013. Prior to this appointment, Sundar Pichai had been in charge of development for Chrome and other Google managers had headed Android development. So while Android is a highly important component of Google’s data acquisition and services strategy, it seems to be clear that Google sees Chrome as the most important tool at its disposal for Web data and services, in part because it is a universal, cross-platform tool and in part because it is focused on eliminating dependencies and interference from device-specific software and services that could compromise the quality or security of such data gathering.

How successful has Google been in penetrating mobile markets with Chrome browsers? The answer to this question is fairly murky, due to the complexities of mobile data traffic measurement and the ways in which Google’s mobile device and partners deploy its software. For example, NetMarketShare measures Chrome’s mobile browser market share at about 2.4 percent as of April 2013. However, there are some key factors that seem to argue for a much stronger Chrome mobile presence today than is indicated by many measurements. First, as of June 2012 new versions of the Android operating system released by Google include Chrome as its default mobile browser. Statistics released by Google this month gauging visits to its Google Play Store service for Android indicate that these more recent versions of Android are deployed on more than 45 percent of mobile devices using the Google Play Store.

Given that Android operates about 80 percent of the mobile phones in the world today and more than half of its tablets, according to most market measurements, it would seem that Google Chrome is available prevalently on Android devices. For Apple devices, there is less direct data available for measurement, but it’s worth noting that more often than not the Google Chrome browser ranks at or near the top of downloaded apps in Apple’s App Store for its mobile devices.

### EXPANDING THE ENVELOPE: OFFLINE CACHING AND CHROME OS

While the browser wars are worth monitoring for key market trends, to some degree the evolution of Google Chrome as a product and a platform is beginning to change the nature of what is being measured. Where most people consider a Web browser to be a container for Web pages that they visit,

increasingly browsers are becoming platforms for very sophisticated software and services, sophisticated enough that they are beginning to replace the need for computer-based operating systems to deliver these sorts of capabilities.

One of the key services promoted by the development of Google Chrome that pushes this concept of “Web services” is the use of the evolving standards for HTML to provide more pervasive and stable use of Web-based software. In HTML 5, the most recent version of the evolving W3C standards for HTML, the concept of offline computing was introduced as a Web standard within browser software. HTML 5 supports offline caching of data associated with a Web page or software on a user’s computer, a feature that works within the secure “sandboxed” programming of a Google Chrome browser.

If a connection to the Web is lost, this caching capability enables the modification of information to proceed, and to be synchronized (“synced”) with the Web-stored version of this information once connectivity is restored. In conjunction with services such as Google Drive’s document storage and editing, this enables software to treat a document or other types of data structures in much the same way that a PC-based software package would treat them, except that there is no exposure of the data to exploits on the computer equipped with Google Chrome.

Many different types of software applications can use this HTML 5 offline caching feature, but Google has maximized its ability to make its Google Drive storage and document editing services useful by the use of offline editing via Chrome. Offline editing can work in other browsers also for Google Drive and other Web apps, but Google has underscored the value of Web-only software by introducing a new kind of operating system: Chrome OS.

Chrome OS uses a Linux-based computer operating system, much like that found on computers and mobile devices around the world. Unlike other computers equipped with Linux or some other operating system, though, Chrome OS offers only Google Chrome as the environment in which people can access software and services. When you log in to a Chrome OS-equipped computer using your Google Account, you see a “desktop” display similar in design to other computer operating system displays, but that desktop is simply a tool to access software and services within Chrome. There is some local storage available for files and portable USB storage media can be attached to a Chrome OS computer, but this is mostly intended for the temporary storage of files uploaded or downloaded via the Web.

Combined with the secure offline data caching capabilities of HTML 5, Chrome OS offers what is arguably the most secure and stable user com-

puting environment available today. There is no malware software specific to Chrome OS, because there is no user software that works on the computer outside of Chrome. Except for the local cache of downloaded files, the file system structure of Chrome OS computers is completely isolated from Chrome OS users, except for those who opt for the Developer’s mode for Chrome OS, which can be enabled only with a hardware switch on the unit. Software launched via Chrome OS always works as user-level software – there is never any access to the operating system as a whole, except via very carefully defined secure software interfaces (APIs).

The independence of Chrome OS from specific devices is underscored by the manner in which it is configured. If you were using a Chrome browser on any desktop or laptop computer prior to using Chrome OS for the first time, upon logging in to Chrome OS you will see every feature of customization and services available on your Chrome browser appear automatically on your Chrome OS computer. If your Chrome OS PC is damaged or lost, upon using a new one everything except files in your local storage will be configured in exactly the same way. In other words, Chrome OS underscores that Google Chrome is a secure, self-contained extension of the Web, no matter what machine that you may use to access it.

This cross-platform universality of the Chrome experience is underscored on Windows PCs now by the option to add the same desktop view components in Chrome on Windows that you find on Chrome OS. In other words, even if you have a Windows PC, in essence you are already running Chrome OS – it just happens to have a less secure computing environment underneath the Chrome app. Microsoft is adding Web-based document editing capabilities also via its online Office 365 services, so Google is not the only company trying to underscore so-called “cloud” computing services. However, unlike Google Drive document editing services, premium Office 365 services require the installation of Microsoft Office software on a PC or Mac running your Internet Explorer browser. These more proprietary premium “hooks” yet again open the door to computer viruses and malware and dependency on hardware that is vulnerable to damage or loss.

While Chrome OS is thought of by many people as a niche product, it’s becoming a much more significant presence in the computer marketplace. Launched first in May 2011 for general sales on Chromebook laptop and Chromebox desktop devices, Chrome OS-equipped computers now account for 20 to 25 percent of all laptops sold today for less than \$300. If one thinks of the market share growth curve for the Google Chrome browser since its launch in 2008 and for Google’s Android

operating system, it's not inconceivable that Chrome OS could operate a majority of desktop and laptop computers sold within the next three years. The potential for this sort of growth is underscored by Google's introduction of the Chromebook Pixel laptop computer earlier this year. The Pixel is a \$1300 touch-screen laptop with a build quality, screen quality and overall performance similar or better than many laptop computers in that price range. While the primary mission of the Chromebook Pixel is to make software developers more interested in creating sophisticated Web apps, clearly the Pixel points to the potential for Chrome being able to satisfy the full range of needs that today's computer users have – with or without typical computer operating systems supporting its functions.

**PUSHING THE ENVELOPE: CHROME ADVANCED FEATURES**

While Chrome OS is an important component for advancing the development of Google Chrome and its open-source Chromium components, Chrome in all of its forms exists primarily as a tool for Google to advance its overall goal of making the Web as a whole a more powerful computing platform. To attain this goal, Google must work constantly to push both the performance of its own software for Chrome and the Web standards that support it. Google does this constantly, contributing significantly to open source standards and to software available on an open source basis to ensure that Chrome is always required to compete with the Web as a whole to provide the best data to Google for its use and analysis.

Google pushes standards and performance in several important areas. One of the most important arenas for improvement is in graphics performance. WebGL, an extension of HTML-based programming that focuses on supporting the capabilities of powerful graphics processors built into today's "system-on-a-chip" computer hardware, is supported and promoted by Chrome developers actively. WebGL provides advanced programming techniques for computer games and other visually-oriented software that requires high performance graphics. The new "Canvas" element for HTML 5 is also an important tool for developing advanced graphics interfaces. The result is a new array of high-performance software applications that are on course to meet the expectations of data-intensive graphics software.

Google has been also developing and promoting Web standards that can free developers from the issues of licensing fees for patents related to specific data formats and software. For example, WebRTC is an open source, real-time communications protocol implemented in Chrome that enables highly efficient, two-way transfer of data and multimedia in real-time communications. Google's own software applications now make extensive use of WebRTC via Chrome, including its popular Google+ Hangouts online video chat and collaboration services. Google Chrome APIs are now available for secure access to the sensors typically found on today's mobile computers. GPS data, gyroscopes, accelerometers, cameras, microphones and other devices, including sensors built into many of these devices as well as a wide range of plug-and-play devices. Both Web RTC and Chrome's

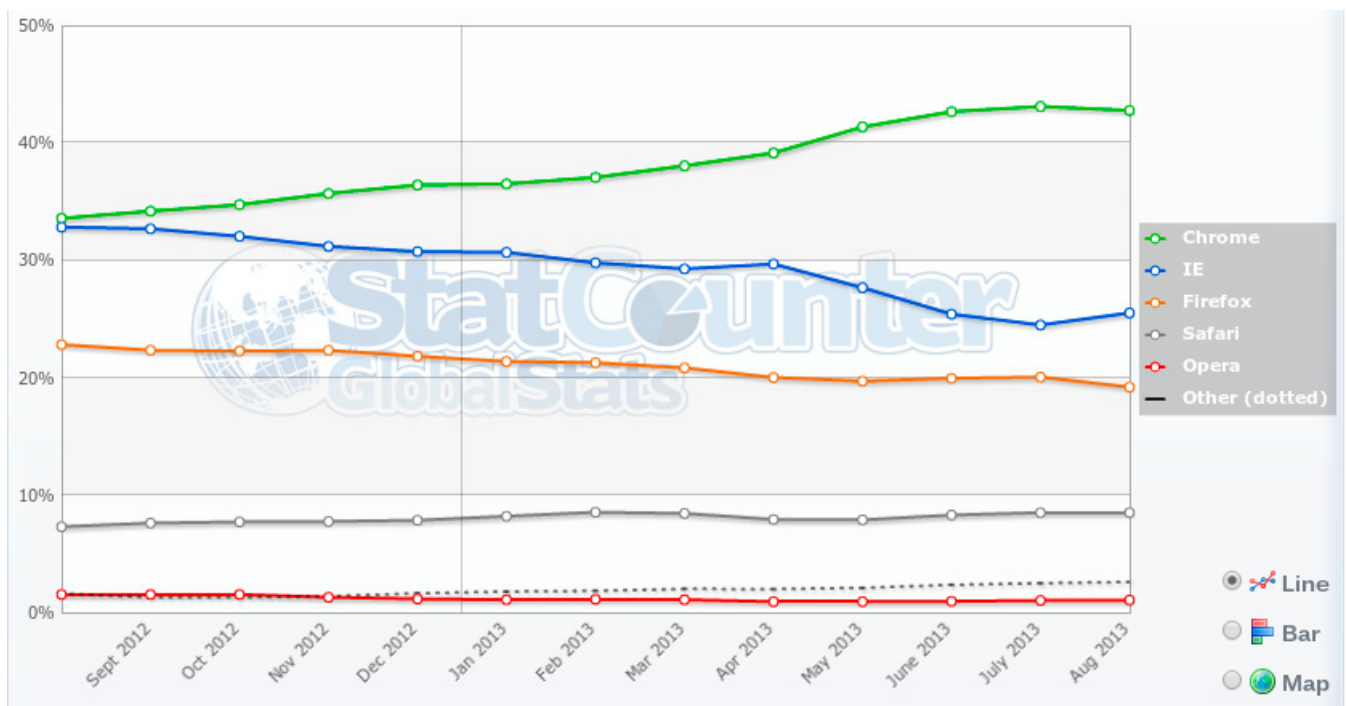
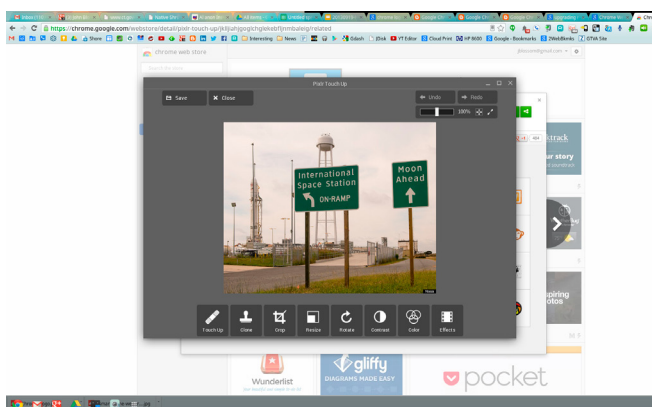


Figure 3. StatCounter Web Browser Global Market Share Statistics

sensor APIs expand the range of data that can be analyzed by Google services, as well as by other Web services providers, providing a more rich experience via the Web that both rivals and sometimes exceeds what we have come to expect from traditional computer software.

Programming languages themselves and the underlying code that drives Web services are also recent targets for Chrome improvements. Earlier this year Google Chrome shifted from supporting WebKit as its Web page rendering engine to a variant called Blink, which is intended to provide key performance in security advantages over time. As with other Chrome components Blink is made available as open source code over time via its Chromium project, but clearly Blink exists to both push the Web as a whole to perform better and to shape how the Web adopts specific standards. Google is also promoting a new Web free and open source programming language called Dart, which helps to improve the performance of Web-based software, and uses Dart actively in Chrome-based apps.

Similarly, Google has been developing and adopting new standards for Web graphics. WebP is an open source image storage standard similar in concept to earlier GIF and JPEG formats, but free of royalties for its use and significantly more efficient in rendering images. WebM for stored video and VP9 for streaming video are Google-developed video equivalents of WebP, offering open use freedom from patent royalties (rights to which were acquired by Google for all WebM users) and more stable and secure control of videos. WebP and WebM support by Chrome ensures that fewer elements of data formatting and use will be constrained by patent rights and will be allowed to be improved in their performance in an open way over time.



**Figure 4.** Chrome App in Windows

The net result of these and other advanced technologies for Chrome have been showcased by Google throughout the years, and the most recent demonstrations of their capabilities have been impressive. At the Google I/O Developers Conference this year, there were demonstrations of Web-

based games using Chrome in which a camera equipped with a motion sensor was used to interpret the movements of a person to simulate sky-diving through a three-dimensional game space on a large screen. Sensor integration, 3D graphics and real-time capabilities all in one demonstration – simple by the standards for some computer game experiences, but impressive by the standard of what has been achieved via Web software.

Other demonstrations of real-time interactivity included Racer, a slot car game that operated on a race track that crossed Chrome browsers on multiple mobile device screens – the ability to create secure, multi-person, multi-screen collaborative experiences in real-time. RollIt is a multi-player demonstration of the classic arcade game of rolling a ball up a ramp into a series of holes – except that a Chrome browser on a mobile phone or tablet acts as the sensor-driven controller to “roll” the ball that appears in a Chrome browser on a laptop or desktop computer as it falls into the ramp’s holes. These are simple demonstrations that target the multi-billion online game industry, but there is a wealth of high-power applications that can make use of these sorts of secure, multidimensional, sensor-driven capabilities.

Secure and simple online entertainment via Chrome is also emphasized in a recent Google product introduction – Chromecast, a \$35 device that plugs into the HDMI port of most modern televisions and that streams content from the Web using apps on mobile phones, tablets and PCs as the controls for these streams. A Chromecast is basically a Chrome browser with an Android operating system stripped of all of the components relating to Android apps, but including Chrome components developed for Android-based Google TV devices to manage television devices. While technically not a Chrome OS device, a Chromecast extends the concept of secure computing by isolating a Chromecast via the secure Chrome computing environment and by relying on the Web for most of its content streaming instead of the mobile device itself. It is possible to stream content stored on PCs via a Chromecast, but currently Google is disallowing this capability in its production versions of the product, allowing only the transmission of images of a Web page in a Chrome browser on a PC or Mac to a Chromecast-equipped TV.

## WHAT IS THE FUTURE OF CHROME?

As you can see, Google Chrome is much more than a browser. It is a complete computing environment that encompasses most of today’s personal computing devices and provides a wide range of sophisticated capabilities. It is expanding the envelope of what we think of as Web-based computing, even as it pushes the range of devices and technologies that are able to communicate with the



Web and with one another via the Web. Increasingly Chrome is our destination for everything that we do on the Web, in large part because it tries to expose the Web in full to people in more ways on more devices than other technology available today. Google may have its motivations for doing so, but those motivations have one goal in mind – a broader and richer Web for everyone.

The future of Chrome is clearly moving beyond the browser itself. Recently Google introduced a program called Chrome Apps. Chrome Apps run via any Google Chrome browser on a PC or Mac or via Chrome OS, but they do not launch as a Chrome browser tab or window. Instead, Chrome Apps launch in an application window without browser controls – in other words, they look and act just as any other app would on a personal computer. To some degree Chrome Apps are simply making the capabilities of Web-based apps look more like traditional computer-installed software – you can download Chrome Apps from the Chrome Store, for example, a Web portal that is available also for installing browser-based Web apps and highly functional Web sites in your Chrome browser for later use.

But whatever the packaging, Google Chrome is telling us something very powerful that needs to be appreciated by more people more fully. Often these days you can hear the phrase, “The PC is dead.” Well, I’d like to suggest that it’s not the PC that’s dead but rather the notion of insecure, isolated and proprietary personal computing that’s dead. Personal computing has never been more valuable, and it’s so valuable because the Web can help a computer to do so much with so many other people so very well. More than any other Web technology in our hands today, Google Chrome advances the concept of the value of the Web, the world and computing being merged in as many useful ways as possible in as many places as possible. For that reason, it pays for us to be very aware of all of the places that Google Chrome points us – and to plan accordingly.

#### ABOUT THE AUTHOR

*John Blossom is a globally recognized content industry analyst, providing thought leadership and improved strategic marketing for executives in search of new approaches to rapidly changing markets for information products and services. Mr. Blossom founded Shore Communications Inc. in 1997, which provides research and advisory services for major and emerging publishers and content technology companies in enterprise and media markets. Mr. Blossom speaks frequently at major conferences for senior industry executives, is quoted often in the press and is the author of the book “Content Nation: Surviving and Thriving as Social Media Changes Our Work, Our Lives and Our Future,” published by John Wiley & Sons.*



### [ GEEKED AT BIRTH ]



You can talk the talk.  
Can you walk the walk?

### [ IT'S IN YOUR DNA ]

- LEARN:**
- Advancing Computer Science
  - Artificial Life Programming
  - Digital Media
  - Digital Video
  - Enterprise Software Development
  - Game Art and Animation
  - Game Design
  - Game Programming
  - Human-Computer Interaction
  - Network Engineering
  - Network Security
  - Open Source Technologies
  - Robotics and Embedded Systems
  - Serious Game and Simulation
  - Strategic Technology Development
  - Technology Forensics
  - Technology Product Design
  - Technology Studies
  - Virtual Modeling and Design
  - Web and Social Media Technologies

# GOOGLE CHROME FORENSICS

by Krystina Horvath

In this article, you will learn about the technical forensic processing of the Google Chrome web browser as used on Linux and Windows operating systems. Privacy issues concerning Chrome and how they are beneficial to forensic investigators will also be discussed.

## What you will learn:

- Google Chrome forensics on Linux operating systems
- Google Chrome forensics on Windows operating systems
- Google Chrome privacy issues

## What you should know:

- Basic understanding of Linux operating systems
- Basic understanding of Windows operating systems
- Basic understanding of Google Chrome web browser
- Basic understanding of binary and bit integers

**W**hy focus on Google Chrome Forensics? This popular website browser is built unlike other popular browsers such as Mozilla Firefox, Safari and Internet Explorer. Although Google Chrome stores browser history in a SQLite database like Mozilla Firefox, there is a significant difference in the structure and number of the SQLite database that Chrome uses.

Similar to other web browsers, Google Chrome saves a variety of information corresponding to prior Internet history activity. Website history including cookies, form history, search terms, bookmarked URLs and downloads are all data that is logged into Chrome's History SQLite database. In Chrome, each operating system stores its History SQLite database in a specific location. Within Linux, Chrome stores its

history files in the following locations: `/home/$USER/.config/google-chrome/` *and* `/home/$USER/.config/chromium/`. And within Windows, Chrome stores its history files in the following locations: `C:\Users\[USERNAME]\AppData\Local\Google\Chrome\` (for Windows Vista and Win 7) and `C:\Documents and Settings\[USERNAME]\Local Settings\Application Data\Google\Chrome\` (for Windows XP).

Google offers two official versions of Chrome for Linux operating systems (one is Google Chrome and the other is Chromium) and Google Chrome on Windows operating systems. This article will expose the technical forensic processing of Chrome on Linux and Windows operating systems. We will begin by uncovering the issues associated with Google Chrome forensics within Linux.

## CHROME CACHE ISSUES IN LINUX

The structure of Chrome is the same on a personal computer as it is on a mobile Android-based device, such as a tablet or smartphone. Unfortunately, the Google Chrome cache presents pertinent issues to forensic investigators. These issues are the following:

- Files stored in the cache do not carry the original file name from the web server, instead, they are renamed
- Text file extensions such as .json and .html are compressed into .zlib files
- Any file smaller than 16,384 bytes are located in container files (also known as block files) which hold several smaller files. Metadata about these files are also stored in the block files through binary indexing.

By renaming the original files, compressing text files and storing smaller caches in a container file, a forensic examiner will not be able to create a clear picture of the Chrome cache in question.

## GENERAL COLLECTION OF CHROME DATA

If a computer forensic examiner would like to simply extract all data from Google Chrome from a

Linux-based operating system, the following command is used to parse the information and create a spreadsheet:

```
hindsight.pl [-i Chrome_History_Data_Directory] [-o
Output_ChromeData].
```

The command, `-i`, tells the machine to pull information from the input directory, `Chrome_History_Data_Directory` while `-o` creates an output name (in this case, `ChromeData`) and uses it in a sqlite file and an .xlsx file (`ChromeData.sqlite` and `ChromeData.xlsx`).

Before running this command, the examiner will need to download and install Perl and `hindsight.v0.82.zip`. Hindsight can be downloaded for free through the following website, <https://code.google.com/p/hindsight-internet-history/>. Hindsight needs to be unzipped and placed in the same directory with `hindsight.pl`.

## CHROME CACHE STRUCTURE WITHIN LINUX

What is a cache? Chrome, like other Internet browsers, stores the files a user views from a website temporarily in a cache on the user's hard drive. From a cache, previously viewed user information can be retrieved which make accessing websites faster when a user visits it a second or third time.

a d v e r t i s e m e n t

# ModelOff 2013

## The Ultimate Financial Modeling Challenge



**\$30,000 First Prize**  
Register NOW at [www.modeloff.com](http://www.modeloff.com)

**S&P**  
CAPITAL IQ

 Microsoft

**Bloomberg**  
INSTITUTE

**MODELOFF**  
FINANCIAL MODELING  
WORLD CHAMPIONSHIPS 2013



The caches Google Chrome creates are stored in one folder known as *cache*. This caching folder is comprised of base files which are four block files and an index file (named *data\_0*, *data\_1*, *data\_2*, *data\_3* and *index*). Downloaded files are stored within a block file while the index file logs the storage location and transaction information of these downloaded files. Block files are stored according to the amount of storage that one block file is assigned to hold.

For example, block file, *data\_1* can hold cache files up to 1,000 bytes; *data\_2* can store up to 4,000 bytes of cache data and *data\_3* can hold up to 16,000 bytes (the maximum amount) of file data. Therefore, a predefined number of caches are dedicated to each block file.

To reiterate, files under a 16,384 byte size are stored in these block files while any files larger than this size are stored outside of the block file. This output can be viewed through the command, `ls -lSr`. The output is depicted in Listing 1.

**Figure 1.** Output of `ls -lSr` Command

```
-rw-r--r-- 1 khorvath 242639 Jul 15 20:08 index
-rw-r--r-- 1 khorvath 1581056 Jul 15 20:08 data_1
-rw-r--r-- 1 khorvath 2105344 Jul 15 20:08 data_2
-rw-r--r-- 1 khorvath 4202496 Jul 15 20:08 data_3
```

One major issue an examiner will experience with Chrome cache structure is when one of these blocks or index files is deleted or corrupted, the rest of the base files are deleted and new files are created. Therefore, any stored caches before the corruption will not be able to be retrieved during a forensic investigation. Each cached file is assigned a 32-bit address which indicates where the cache is stored (this will be in little-endian format). This allows computer forensic examiners easy identification of the locations of these files, whether they are within block files or stored outside of the block files and other metadata, such as http headers, entry name and request data.

It is critical to understand the structure of this 32-bit address in order to recover information about the cached files. The beginning four bits of these 32-bit addresses expose the header of the cached file. The remaining 28-bits indicate the file type. These file types can be separate files (larger than 16,384 bytes) or block files. The first four bits of these addresses are interpreted in the following Table 1.

Through identifying and interpreting the cached files according to the preceding method, a forensic examiner will be less likely to overlook detailed information within these files. Due to the complex Chrome cache structure on Linux operating systems, a computer forensic examiner must research

and have a firm understanding of bit-integer and binary numbers as well as what the interpretation is for each number within these cached files.

## GOOGLE CHROME DOWNLOAD HISTORY ISSUE WITHIN LINUX

Google Chrome poses an interesting issue regarding download history through the browser. Instead of storing the downloaded history in a separate file, Chrome places the download history in the SQLite database along with the Internet history. In Linux, these download history files can be found in the file path, `/home/.config/chromium/Default`. There are a total of nine SQLite history tables; downloads, keyword search terms, meta, presentation, segment usage, segments, URLs, visit source and visits. In this instance, we will focus on the download SQLite table.

## SQLITE DATABASE STRUCTURE

The SQLite databases where this data is stored are meant to analyze and display the information from the database in a relational manner. These tables are useful for a general overview of Google Chrome artifacts within Linux. However, they do not give fully accurate information because there is little segregation between the information stored in the SQLite database. Unless a computer forensic examiner knows where to locate specific files and data, pertinent information to a case may be completely overlooked during a Google Chrome artifact investigation.

Even though the SQLite database structure is complex within Google Chrome, there are two clues that an examiner can search for to determine how the tables within the database relate to one another and analyze the output. One clue that SQLite databases offer are SQL view statements. View statements are virtually created tables that pull information from other tables in the database. These statements allow the Chrome user to bypass retyping a frequently used query. In essence, these view statements have an intended use by the creator. By examining these view statements, inferences can be made dependent upon the data frequently queried.

The other clue uses a simple approach to understand the relation between tables within the

**Table 1.** Binary and Integer Interpretation of Cached File Types

Binary	Integer	What it means
000	0	Separate file
001	1	Rankings block file
010	2	256 byte block file ( <i>data_1</i> )
011	3	1k block file ( <i>data_2</i> )
100	4	4k block file ( <i>data_3</i> )



database. Table and field names are critical indicators of interrelationships of tables embedded in a database.

For example, a database file named “Indexed-DB.db” will contain information from a “Stored Object” table and an “Images” table. In this case, the common field for this database is the object identification number. In turn, this is helpful in two instances. One instance is during investigation of the SQLite database queries created by the user. This will indicate to the examiner which information has been queried and most frequently used. Another instance to use this information is when the examiner wants to cross reference two tables to gain a better understanding of what kind of browsing, downloading, form history and caching was completed over the user’s duration of machine use.

## CHROME DOWNLOAD HISTORY FORENSICS METHOD WITHIN LINUX

In order to extract Google Chrome downloaded files, a grep command can be used in the Linux terminal. A simple command, `sqlite3 History .schema | grep downloads`, will extract the Chrome downloaded files into a table format. However, the date and time are in Unix Epoch format (the number of seconds that have elapsed since the time 00:00:00). An examiner will experience difficulty in pinpointing the local time. To remediate this issue while creating a CSV formatted table with the extracted download history with the ID, file path, URL address and date (in local time), an examiner can use the command:

```
sqlite3 History .schema | grep downloads -header
-csv History "SELECT id,full_path, url,
datetime(start_time,'unixepoch','localtime')
FROM downloads".
```

The output for this command is shown in Listing 2.

### Listing 2. Google Chrome Download History Output

```
id,full_path,url,date,received_bytes,total_
bytes,state
1,/home/khorvath/Downloads/Redline-
1.8.msi,http://www.mandiant.com/mandiant/
download/Redline-1.8.msi,"2012-05-04
19:94:59",500022,500022,complete
```

## CHROME SESSION AND TAB FILE FORENSICS

This section will focus on investigating Chrome history in the form of *Current Tabs*, *Current Session*, *Last Tabs* and *Last Session*. The information stored in these sessions and tabs allows Chrome to restore previous browsing sessions in the event

of a browser crash or accidentally close out of the session. These tab and session files hold a plethora of significant data but the file format poses a problem to computer forensic examiners. This issue pertains to file structure and source code of the data in these session and tab files.

In order to grasp the structure of these files (*Current Session*, *Current Tabs*, *Last Session* and *Last Tabs*), the files should be opened in a hex viewer, such as DHEX. Once the hexadecimal values are exposed, deciphering the file structure is fairly simple. The header is found within the first 32-bit integer. SNSS is a common file signature (53 4E 53 53 – first four-bit integer within the hex of the file) that corresponds to the *Session Backend* portion of the *Current Session* or *Last Session* files. Within these session files, each record is logged as a sixteen-bit integer to indicate the byte size of the record and a remaining eight-bit identification to indicate the type of record. After that, the session contents were displayed in the hex, as well. Therefore, the file structure of these session files is the following: size of record, contents of record, size of next record, contents of next record and so on.

Since the file structure has been defined, the content structure within these session files is a little more complex.

- The *Session Backend* file operates with a *Session Command* object, which is also used on *Tab Restore Service* and *Session Service* to disclose the disk state.
- The *Tab Restore Service* and *Session Service* use a common field of *Base Session Service*. Within this *Base Session Service* file, a technique is used called *Create Update Tab Navigation Command* that writes all data about sessions and tabs into the *Session Command* file.
- The data written into the *Session Command* starts with a 32-bit integer that gives the length of the recorded data. The rest of the *Session Command* structure is depicted within the following Table 2.

When following this content structure, an examiner can thoroughly and accurately extract session and tab data from Google Chrome.

## CHROME FORENSICS IN WINDOWS OPERATING SYSTEMS

Although the SQLite database structure is the same as on Linux, Windows operating systems allow a computer forensic examiner to utilize GUI-based forensic tools such as ChromeForensics by woanware to extract Internet artifacts. This tool is available for Windows 2000, XP, Vista, 7, Server 2003 and Server 2008 operating systems. ChromeForensics supports Chrome versions 1 through 27

and newer versions are added. This tool can be downloaded through <http://www.woanware.co.uk/forensics/chromeforensics.html> as freeware.

ChromeForensics extracts several facets of Internet artifacts including downloads, login information, visited websites, bookmarks, cookies, search terms and caches. ChromeForensics features report generation of Internet artifact in XML, CSV and HTML format.

Once the program is opened, a forensic examiner must choose the file path where the files are stored. In this case, it will be `C:\Users\Default\AppData\Local\Google\Chrome`. After the examiner loads the profile, the extraction will format the information into eight tabs (visits, keyword search terms, downloads, auto fill, cookies, favicons, thumbnails and history index).

## GOOGLE CHROME CURRENT PRIVACY ISSUES

What are the privacy issues associated with Google Chrome?

- The Chrome history search feature allows all “secured” information such as financial institution passwords available without visiting the secure website.
- Chrome records and keeps form history and other sensitive content where the website it was originally entered in or found on is not needed to pull it up to view again.
- Is this the only issue with sensitive information in Chrome? The answer to this question is no. Google uses their Omnibox, which is not only the address bar to type URLs into but it also

suggests other search terms...and logs the information typed into this address bar and stores some of this information at Google headquarters. Not only does Google Omnibox store and allow Google employees to view sensitive data but other Google services such as Gmail, Google Calendar and Google Docs are all storing the data in an unsecured fashion.

In order to avoid sensitive information being sent to Google through Omnibox, a user can turn off the auto-suggest feature or use a different Internet browser.

## SUMMARY

In conclusion, Google Chrome presents several issues to computer forensic investigators and users. During a forensic examination of Chrome artifacts, an investigator must be aware of the SQLite database structure and exactly how to extract, analyze and manipulate this data within Linux operating systems. A Google Chrome user will experience privacy breaches affecting any sensitive data that they may input into a search or form on a secured website. The methods suggested in this article will aid the computer forensic examiner in extracting information and the Chrome user to protect their sensitive information.

**Table 2.** Session Command Content Structure

Data Type	What does it mean
Second 32-bit integer	Tab Identification
Third 32-bit integer	Tab's back-forward list index
ASCII String	URL of the webpage
UTF-16 String	Title of the webpage
Byte String	Current state of the webpage
Fourth 32-bit integer	Transition type
Fifth 32-bit integer	This integer will be one if the page has post data. If there is none, it is zero
Second ASCII String	Referrer URL
Sixth 32-bit integer	Referrer's policy
Third ASCII String	URL of the original webpage (this is significant if there was a redirection of the URL)
Seventh 32-bit integer	This integer will be one if the user was overridden. If not, the integer is zero

## ABOUT THE AUTHOR



*Krystina Horvath, MBA is currently in the midst of a career change from finance to computer forensics. Krystina is working on her capstone project for Utica College's Master of Science in Cybersecurity program. The topic for this paper focuses on proving the success of malware used in corporate and governmental cyber espionage attacks. Krystina also offers recommendations for security measures to help prevent malware attacks against these entities.*

Recommended

# Automatically Fix Common Windows Problems for Free

Wise PC 1stAid is a trouble-shooting freeware to help fix common Windows problems in an automatic manner. With it, you can say bye to the following & further unlimited problems:

Icon errors, broken links, unable to open regedit/task manager/webpages, slow internet connections, slow startup, slow PC...



WiseCleaner

## Wise PC 1stAid

- ✓ Easy to Match Problem
- ✓ Fast, Automatic & Intelligent Fix
- ✓ In-time, Unlimited & Active Enrichment
- ✓ Unlimited Technical Support



Highly Reviewed by  
Professionals

Official Website for More Information:  
[www.wisecleaner.com/wisepc1staid.html](http://www.wisecleaner.com/wisepc1staid.html)



Support system:  
Windows XP, Vista, Win7/8  
(both 32-bit and 64-bit)

# CHROME FORENSICS HOW TO TRACE YOUR INTERNET ACCESS BEHAVIOR

by **Marcelo Lau, Nichols Jasper**

This article describes computer forensic procedures for discovering Internet Browsing habits, and compiling computer user profiles. This paper suggests useful information regarding the type of information, and how Chrome defaults' directories are used, and what kind of browsing information may be recovered from computers. Simplifying collection and some reporting tools are described.

## What you will learn:

- Understanding Chrome's file structure and the types of data stored.
- How to recover and preserve content using automated tools, and presenting evidence for forensic purposes.

## What you should know:

- Internet Browsing and Navigation History Basics.
- Chrome browser functions such as Clear Browser Data, and Incognito Mode.
- Windows platform installation and embedded Windows applications.

**G**oogle Chrome is an Internet Browser developed by Google, publicly available since December 2008. According StatCounter (see *On the Web* section) browser statistics, Google Chrome is the most worldwide used Browser with almost 37% from the browser market share, followed by Internet Explorer (30%) and Mozilla Firefox (22%). A breakdown of this market share is proportionally reflected in the distribution of user behavior and web site use, as well as the most likely pattern of malicious and fraudulent user habits with attempts to violate security protocols. As a result, Google Chrome opens-up as forensics-targeted software. This article relates several free tools and their usage, used in collecting and organizing the most relevant data inside Chrome's structure presented in easy procedures.

## INTERNET BROWSER FORENSICS

During digital investigations, web-browsing activity often provides useful information covering a particular investigation scope; this because browsers do most Internet registered activity. There is an increase in computer usage (tablets, smartphones, personal computers and related technologies), and most user activities are potentially digital evidence. It is vital for digital forensics investigators, to be able to preserve these files through a legally valid acquisition procedure. Then after extracting this data, it is analyzed and evidence is presented accordingly, in an understandable forensic report format.

- According *Oh, Lee & Lee* (see the link for paper in *On the Web* Section), searching for evidence

left by Web browsing activity is a crucial component of digital forensic investigations. Almost every movement a user performs activity while using a Web browser, leaves a digital trace on the computer. Therefore, when an investigator analyzes the suspect's computer, this evidence can provide useful information. After retrieving data such as cache, history, cookies, and download lists from a suspect's computer, it is possible to analyze this evidence for Web sites visited, time and frequency of access, and search engine keywords used by the suspect.

- Timeline analysis is another useful data capturing method, attempting to find a computer forensic procedure involving web browser activity. When we are trying to find evidence in a timeline, data and time of events are critical in detecting the movement of a suspect along a timeline. The chronology of events is crucial in linking server logs considering application; database or server logs looking for a specific transaction.
- Let us go deeper into Chrome file structures, and examine some useful tools used to mine these precious secrets kept in browser files.

### CHROME FILE STRUCTURE

This article relates a Google Chrome analysis considering the version 28.0.1500.63 m installed on Windows 8 Professional. The file structure can vary on different versions, but this methodology may be applied on several current Google Chrome browser's versions actually used by most computer users.

Chrome stores the user's browser history into a SQLite database like Firefox does. The following locations are the default environment where Chrome keeps the data. Considering some different operating systems:

- Linux: /home/\$USER/.config/google-chrome/
- Windows 7 and 8: C:\Users\[USERNAME]\AppData\Local\Google\Chrome\
- Windows XP: C:\Documents and Settings\[USERNAME]\Local Settings\Application Data\Google\Chrome\

This article mainly focuses on SQLite files used by Chrome Browser's. Other databases files may have importance for forensic analysts. We will use a SQLite Database Browser tool for opening and processing these files. Bookmarks have significant file content too, but their format is not in SQLite; therefore, this article will not focus on JSON (Java Script Object Notation) analysis, or other Chrome data not in this format type.

Let us detail the user directory structure in Windows 8, and their respective files inside the User Data folder (main structure where Chrome's

browser files are recorded): Figure 1. The contents that may be found in this folder are the list of revoke digital certificates and some of Chrome's browser configurations. The most important content may be found inside the /User Data/Default/ folder; here, we find the files, sorted by file size as seen at Figure 2.

Most filenames are self-explanatory regarding the content they reveal. These files offer friendly accessed using a SQL Database tool, because Chrome's browser organizes the files (Chrome's browser objects) with the most important content, and are highlighted.

### HISTORY

This file contains the Browser history and its details (some information about this content may be seen at Figure 3). This file is the most important on

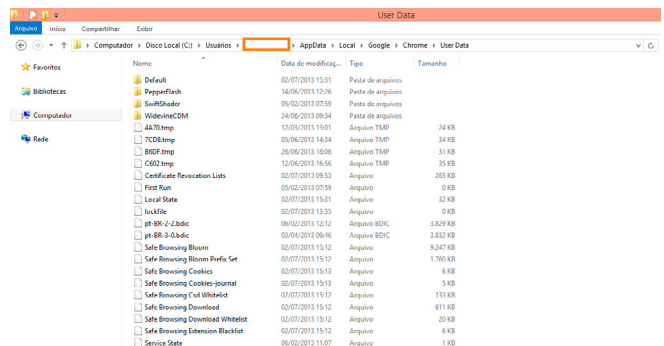


Figure 1. Files inside Google Chrome Folder

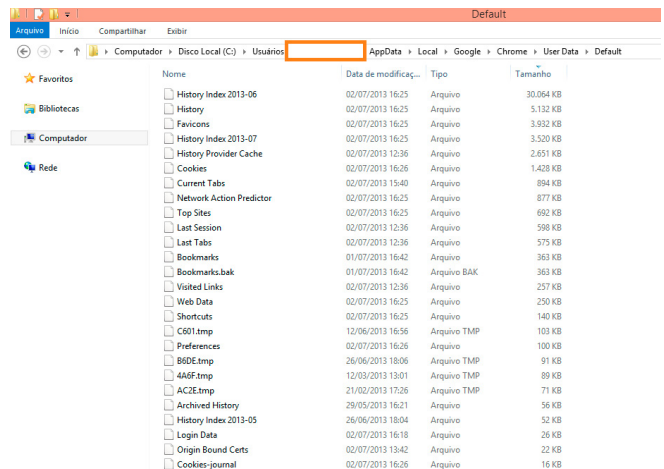


Figure 2. Chrome User Files classified by size

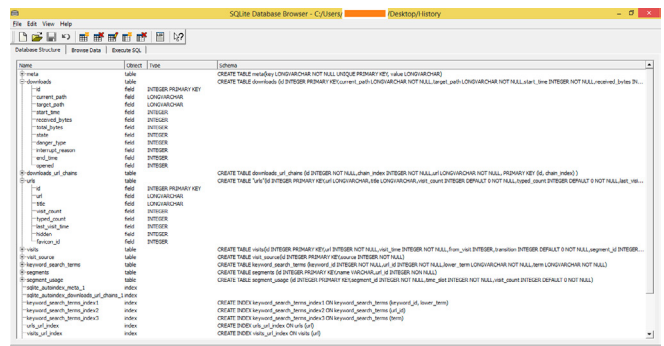


Figure 3. History database table structure

a Chrome Forensics investigation. In your content, we find the history of visited URLs, downloads records and keyword search at Google site. All this information may be crossed to collect more intelligence about a forensics investigation.

## COOKIES

This file contains the cookies where websites transfer some information to the client browser; this data may reveal some control and session content, allowing websites access to some information about the client browser user. Webpages do not store information about a user, if the client browser does not register, or keep any information about any previous access, the user will be treated by the website as a completely new visitor. Special Session Cookies enables the website you are visiting to keep track of your movements inside the site. (Related content about this data recording may be seen in Figure 4). This database will reveal all information about stored cookies: like host data, cookie values, security flags' presence (secure and http-only) and expiry time, among other data. This information may even be considered for investigation purposes. Consider your need to determine if one website is vulnerable or not for session management issues and those cookies may be used to impersonate a previous authenticated user on a vulnerable system. This is a common problem, and the OWASP (Open Web Application Security Project) deems it as one of most critical flaws in web applications last year. For more information, read the link located at "On the Web" section.

## TOP SITES

This file contains most visited websites, and contains some information about their thumbnails. Although it may reveal the same information using filters on the History file, it is different from the history content, top sites organizes this information considering websites information and related user information (Figure 5).

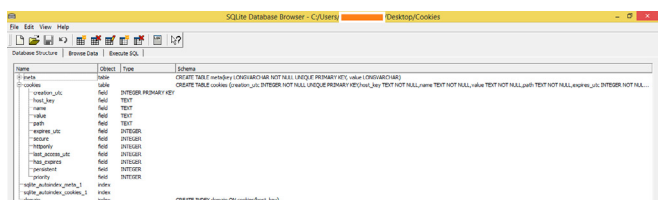


Figure 4. Cookies database table structure

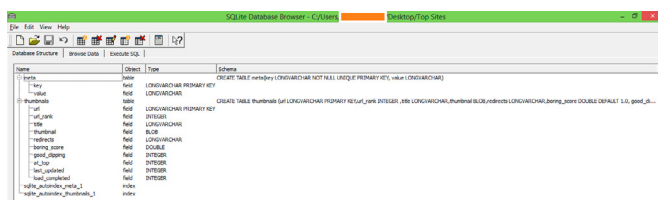


Figure 5. Top Sites database table structure

## NETWORK ACTION PREDICTOR

Aggregates all keywords, or partial keywords, typed by any user on Chrome's browser. It tried to predict what the user is intending to access, giving priority to bookmarked pages, or pages located at history file. This kind of information is not one of the most important in Chrome forensics, but can assist us in understanding the context, or resolve any doubt of what kind of stuff the investigated user was doing in Internet (Figure 6).

Now, it is important to consider where Google Chrome files are located, and how to focus any investigation, or effort in carving relevant data for forensics purposes. Accessing it file-by-file may be difficult or boring; the next article section introduces some tools where they may automate these forensics tasks.

## CHROME FORENSICS TOOLS

This section presents some free tools and may help any forensics investigator searching inside Chrome files and recover important information. Several commercial tools offer alternatives to retrieve web information (for example Internet Evidence Finder, ChromeAnalysis Plus, Oxygen Forensic Suite, etc.). In this article, we will focus on some free tools to help you.

First, let's consider NirSoft Tools. This article demonstrates two tools available at page – [http://www.nirsoft.net/web\\_browser\\_tools.html](http://www.nirsoft.net/web_browser_tools.html) – *ChromeCacheView* and *BrowsingHistoryView*. The download is straightforward, and all tools are portable. Installation or registering is not required; this is perfect for Computer Forensics Investigators because it does preserve all environments; thus, avoiding any system permanent storage contamination.

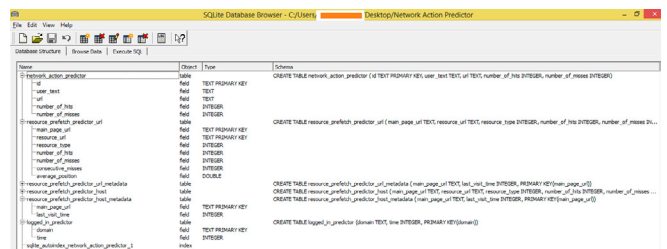


Figure 6. Network Action Predictor database table structure

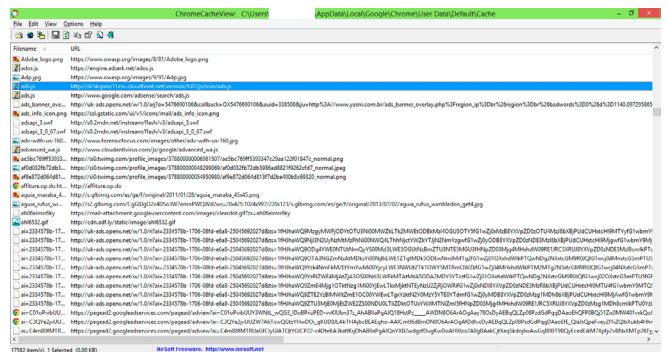


Figure 7. ChromeCacheView results

At first will be demonstrated the Chrome-CacheView test to retrieve some content from Chrome cache files. Click over the Chrome-CacheView tool, and give a double-click on the interface. It may take a while to open, according to cache file's size (Figure 7).

Some filters may sort contents by file type, allowing the tools action when it has selected a file as demonstrated below (Figure 8).

Cache files are a good resource when web browser's temporary files are relevant. Some examples includes cases as collection procedures for pedophilia's suspect, or to determine if an Internet user had access to confidential content at an Internet website.

This tool allows exporting results to a HTML Report using the menu *View* and option *HTML Report* command.

Cache may be relevant, but when investigation involves web browser analysis, history may be an excellent approach. An excellent free tool is *BrowsingHistoryView*, automating your investigation process. Let's start it with a double click in the application icon. The following interface to configure the tool will be seen: Figure 9.

You have the option to set a specific time when the search will be conducted, and the web browsers

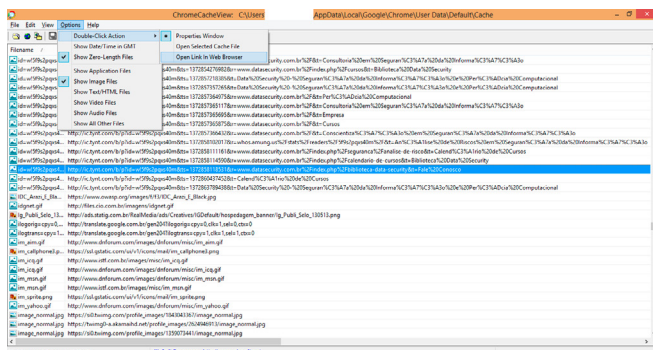


Figure 8. ChromeCache view filters

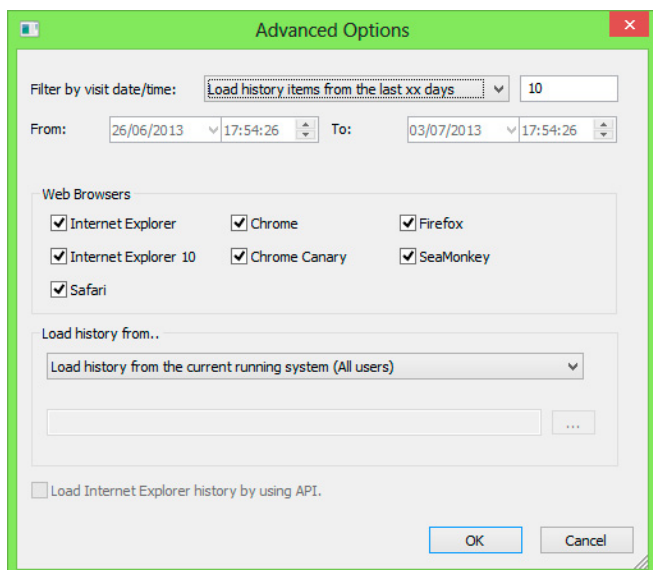


Figure 9. BrowsingHistoryView configuration options









- One important hint is that Incognito mode only keeps Google Chrome from storing information about the websites you have visited. The websites you visit may still have records of your visit. Any files saved to your computer or mobile devices will remain.
- For forensics purposes, let's test if anything is recorded or can be recovered by a forensic expert. If that hypothesis is confirmed, Incognito can be a valuable anti-forensics technique for Chrome users.
- To validate this hypothesis we will build one scenario, following these steps chronologically:
  - Used a Windows 7 Machine with Google Chrome installed.
  - Cleaned all stored data (Ctrl + Shift + Del shortcut).
  - Browsed common websites in Incognito mode during five minutes
  - Use the BrowsingHistoryTool to try to locate log files at Chrome's default directory. Here we have the screen before cleaning process: Figure 20.
- Here we have the screen before cleaning process. After we clean the browsing data, and after using Chrome on websites during a five minutes period, the results are the same. Our forensic tool cannot recover any traces of the user on the web (Figure 21).
- Like an Anti-forensics technique, Incognito represents a challenge. Deleted files can be recovered through data recovery algorithms, but in that case the information aren't recorded by the browser. With this scenario we will need another element to analyze the web behavior from suspect, like proxy, firewall or ISPs (Internet Service Providers) logs that will tell us about sites accessed from a determined station.

## CONCLUSION

Browser log files are very important evidence, needed in many digital forensics investigations.

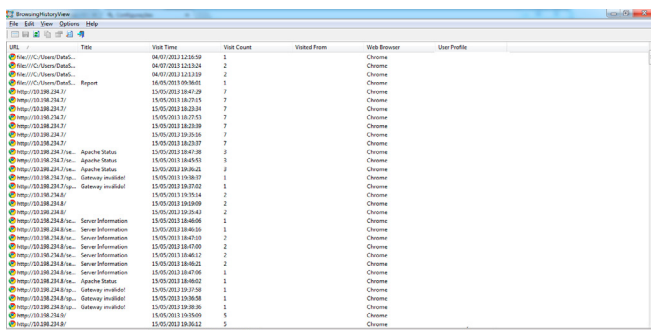


Figure 20. BrowsingHistoryView before cleaning process

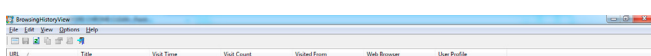


Figure 21. BrowsingHistoryView after cleaning process and five minutes browsing in Incognito Mode

## ON THE WEB

- <http://computer-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/> – Google Chrome Forensics
- <http://www.dfrws.org/2011/proceedings/12-344.pdf> – Oh, Lee & Lee – Advanced evidence collection and analysis of web browser activity – Elsevier
- <http://gs.statcounter.com/#browser-ww-monthly-201206-201306-bar> – Top 5 Browsers from June 2012 to June 2013
- [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) – OWASP TOP Project
- [http://www.nirsoft.net/web\\_browser\\_tools.html](http://www.nirsoft.net/web_browser_tools.html) – NirSoft Web Browser Tools
- <https://www.mandiant.com/resources/downloads/> – Mandiant Forensic Software
- <https://support.google.com/chrome/answer/95464?hl=en> – Incognito mode (browse in private)

After analyzing a web browser usage's trace, we may determine the suspect's behavior, their activities, and their techniques and objectives. It can lead to an attack pattern when we are conducting some security incident forensic response.

Google Chrome forensics tools may assist us to discover some hints inside large amount of evidence filtering by file type, keywords and so on. Analyzing the timeline of browsing can reveal what the suspect did in a specific time, maybe answering some questions about a specific case.

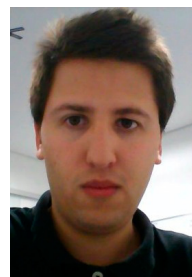
With Internet's continuous spreading through the world, and Google Chrome's consolidating as the leader in the Browser Software Market, Google Chrome Forensics abilities will be a recurrent requirement for the computer forensics investigator. Know where the files are located, and preserve the logs, they can be an invaluable resource to help the expert to uncover the traces, and confirm an investigation line to close the case.

## ABOUT THE AUTHOR



Marcelo Lau is Engineer, post graduated In Administration, Communication and Art. Msc at University of São Paulo and experienced Information Security and Computer Forensics on several large banks in Brazil. Nowadays is owner and executive director at Data Security in Brazil. Well known professor at several universities in Brazil and other South America Countries, as Argentina, Bolivia, Colombia, Paraguay and Peru.

## ABOUT THE AUTHOR



Nichols Jasper is a security analyst with over five years of experience in consulting services, including collection and analyze of many cases of security incidents that demand forensic procedures. The main subjects of investigation is corporate fraud involving intellectual property events and lawsuits that involves the use of electronic evidence in the investigative context.

# 9th Annual International Conference on Global Security, Safety and Sustainability

Williamscollege.co.uk/icgs3-13

4-6 December 2013

**All accepted papers will be published in the International Journal of Electronic Security and Digital Forensics (IJESDF) published by Inderscience ([www.inderscience.com/IJEDS](http://www.inderscience.com/IJEDS))**

In an era of unprecedented volatile, political and economic environment across the world, computer based systems face ever more increasing challenges, disputes and responsibilities and while the Internet has created a global platform for the exchange of ideas, goods and services, however, it has also created boundless opportunities for cyber-crime.

This Annual International Conference is an established platform in which security, safety and sustainability issues can be examined from several global perspectives through dialogue between academics, students, government representatives, chief executives, security professionals, and research scientists from the United Kingdom and from around the globe.

The three day conference will focus on the challenges of complexity, rapid pace of change and risk/opportunity issues associated with the 21<sup>st</sup> century living style, systems and infrastructures.

**Topics: The list of topics includes (but not limited to):**

- Cyber crime, detection, prevention
- Security audit, risk and governance
- Computer forensics and anti-forensics
- Strategic approaches to security
  - Internet fraud, Data Security
- Security Requirements Engineering
- eGovernment/ mGovernment Security
- Network security
- Software Protection
- Attack pattern recognition
- Security in Mobile Platforms
- Systems Safety and Sustainability
- Privacy preserving systems
- Anonymity metrics
- Privacy enhancing location and mobility management
- Transparency and accountability in data protection
- Privacy impact assessment methodologies
- Web 2.0 privacy
- Cyber War
- Criminal data mining
- Security attack ontology
- Infrastructure security

## **Workshops**

- 1) **Cyber Infrastructure protection workshop**
- 2) **Intelligent management workshop**
- 3) **Digital forensics workshop**
- 4) **IT and Cyber Crime law workshop**
- 5) **Security audit, risk and governance workshop**
- 6) **Systems Security, Safety and Sustainability**

Williams College  
London, England

# SAFARI BROWSER FORENSICS ARTIFACTS ANALYSIS

by Mr. Darsh Patel, Dr. M. S. Dahiya, Dr. J. M. Vyas

Apple Safari is the default web browser on Macintosh Systems. The following are key Safari plist files which can give lots of artifacts related with the browser usage and forensic evidences. bBookmarks.plist, TopSites.plist, History.plist, LastSession.plist. These files can be located at ~/Library/Safari/. Cache.db, Cookies.plist.

#### What you will learn:

- How Safari Browser stores the artifacts.
- Safari Browser & URL
- Safari artifacts locations
- Plist file & its basics
- From where the artifacts came out

#### What you should know:

- Unix Timestamp calculation
- Opening Plist with terminal
- Unix basics operations

It is very significant for forensic experts to note the “private browsing” feature and its influence on these artifacts.

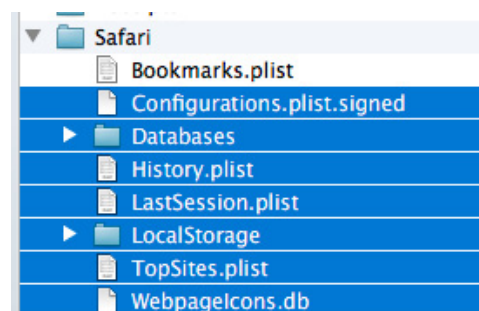


Figure 1. Safari Browser Plist Files

#### WHERE TO LOCATE THE EVIDENCE FILES IN SAFARI BROWSER?

Artifacts related with Safari browser running on Mac OS X 10.8 are as follows:

- TopSites: /Users/<username>/Library/Safari/TopSites.plist
- Bookmarks: /Users/<username>/Library/Safari/Bookmarks.plist
- History: /Users/<username>/Library/Safari/History.plist
- Cookies: /Users/<username>/Library/Cookies/Cookies.binary-cookies
- Last session: /Users/<username>/Library/Safari/LastSession.plist
- Cache: /Users/<username>/Library/Caches/com.apple.Safari/Cache.db

Other Artifacts can be also considered:

- Downloads: /Users/<username>/Library/Safari/Downloads.plist
- Extensions: /Users/<username>/Library/Safari/Extensions/Extensions.plist

- Webpage Icons: /Users/<username>/Library/WebpageIcons.db
- Webpage Preview (thumbnail): /Users/<username>/Library/Caches/com.apple.Safari/Webpage Previews
- Local storage: /Users/<username>/Library/Safari/LocalStorage/ and /Users/<user>/Library/Safari/LocalStorage/StorageTracker.db
- History Index: /Users/<username>/Library/Safari/HistoryIndex.sk

## FORENSIC ANALYSIS OF PLIST FILES

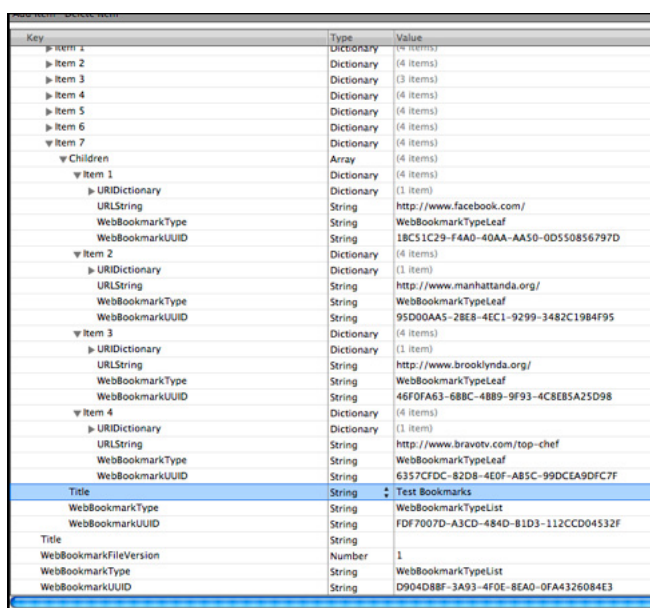
### TOPSITES.PLIST

What is this plist file? TopSites is a fresh feature that gives a view of some of maximum visited sites by the user. Inside the browser, the top websites visited may be very useful for an examiner. Reading through the plist file is quite instinctive. A user can edit their top sites and either marks a site as “pinned” or forever removed from the top sites list. When a site is marked as pinned, and then it will be forever included in the list until the user selects to reset the top sites list.

The plist file does not provide a time stamp of when an entry is added to the file but there are xml tags that indicate the last modified date/time of the file embedded within the file itself. Based on tests it seems that the file is appended with entries. For example, visiting a website multiple times (even after restarting the application) does not guarantee a website to be included in this file. However, the plist file may be updated several minutes later to include top websites visited.

### BOOKMARKS.PLIST

This is a binary plist file used to store Safari bookmarks. By default, Safari will have some websites included in the Bookmarks.plist file. These built-in



Key	Type	Value
Item 1	Dictionary	(4 items)
Item 2	Dictionary	(4 items)
Item 3	Dictionary	(3 items)
Item 4	Dictionary	(4 items)
Item 5	Dictionary	(4 items)
Item 6	Dictionary	(4 items)
Item 7	Dictionary	(4 items)
Children	Array	(4 items)
Item 1	Dictionary	(4 items)
URIDictionary	Dictionary	(1 item)
URLString	String	http://www.facebook.com/
WebBookmarkType	String	WebBookmarkTypeLeaf
WebBookmarkUUID	String	1B51C29-F4A0-40AA-AA50-0D550856797D
Item 2	Dictionary	(4 items)
URIDictionary	Dictionary	(1 item)
URLString	String	http://www.manhattanda.org/
WebBookmarkType	String	WebBookmarkTypeLeaf
WebBookmarkUUID	String	95D0AAS-2BE8-4EC1-9299-3482C1984F95
Item 3	Dictionary	(4 items)
URIDictionary	Dictionary	(1 item)
URLString	String	http://www.brooklynnda.org/
WebBookmarkType	String	WebBookmarkTypeLeaf
WebBookmarkUUID	String	46F0A63-68BC-48B9-9F93-4C8E5A25D98
Item 4	Dictionary	(4 items)
URIDictionary	Dictionary	(1 item)
URLString	String	http://www.bravotv.com/top-chef
WebBookmarkType	String	WebBookmarkTypeLeaf
WebBookmarkUUID	String	6357CFDC-82D8-4EDF-AB5C-99DCEA9DFC7F
Title	String	Test Bookmarks
WebBookmarkType	String	WebBookmarkTypeList
WebBookmarkUUID	String	FD7007D-A3CD-484D-B1D3-112CCD04532F
Title	String	
WebBookmarkFileVersion	Number	1
WebBookmarkType	String	WebBookmarkTypeList
WebBookmarkUUID	String	D904DBF-3A93-4F0E-8EAD-0FA4326084E3

Figure 2. Bookmarks.plist

bookmarks will also be located in the Bookmark menu bar. The user may choose to add new bookmarks to the existing “Bookmark Bar” folder or any subfolders that is created. Note that some users may accidentally add it to the “Top Sites” folder in which case the bookmark will not appear in the Bookmarks.plist file.

If the user chooses to sort / group their bookmarks into folders, then the individual bookmark entries will be grouped together as an array of objects in the plist file, with the folder name included. Below is a screenshot of the bookmarks.plist file containing a folder called “Test Bookmarks” with 4 entries. Notice that the individual bookmarked sites are subitems within an array of objects belonging to that “Test Bookmarks” folder or list: Figure 2.

Inside the bookmarks.plist file, each record will have a WebBookmarkUUID with a corresponding 32 character hex value. Using that WebBookmarkUUID, a corresponding file can be found using that 32 character value as the file name with a file extension of “.webbookmark”. Each webbookmark file is a bplist (binary property list) file holding the URL of the bookmark. Note that the bookmarks.plist file does NOT contain the date/time when the entry was added.

### HISTORY.PLIST

The history.plist file holds a list of web sites referred with the corresponding date/time as well as visit count. Experiments specify that this file is attached at the head / top of the file with the most recent URL referred. The date/time is in MAC absolute time and will need to be decoded.

For each entry in the history.plist file, there is a corresponding web history file located at ~/Library/Caches/Metadata/Safari/History. This web history file can be opened using the default plist editor to analyze out the URL. When history is cleared (not empty cache), the web history files are erased and the History.plist file is resized to 0 bytes.

### IMPORTANT FEATURE

A new “feature” in Safari is to create a snapshot / thumbnail of the website and kept in ~/Library/Caches/com.apple.Safari/Webpage Previews. This is on by default. These are JPEG & PNG files with the same file name but different extension. When the history is cleared, the preview pages will also be deleted unless they are related to bookmarked websites.

### COOKIES.PLIST

The cookies.plist file is located at ~/Library/Cookies/ subfolder. This is a standard plist file and can be simply reviewed. This file can be examined quickly for some indication of websites referred, date/time, as well as latent account names.

## LASTSESSIONS.PLIST

This plist file records the current state of the browser. This plist is used to restore the state of the browser in the event that Safari browser exit unexpectedly. In my lab simulation, if Safari browser is exit as normal, there will be no entry in the SessionWindows

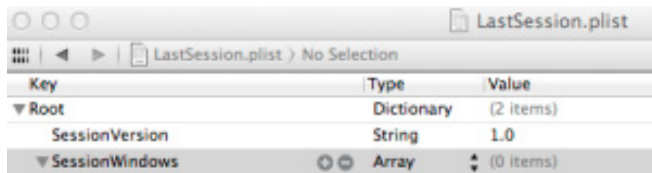


Figure 3. Browsing session ended as normal

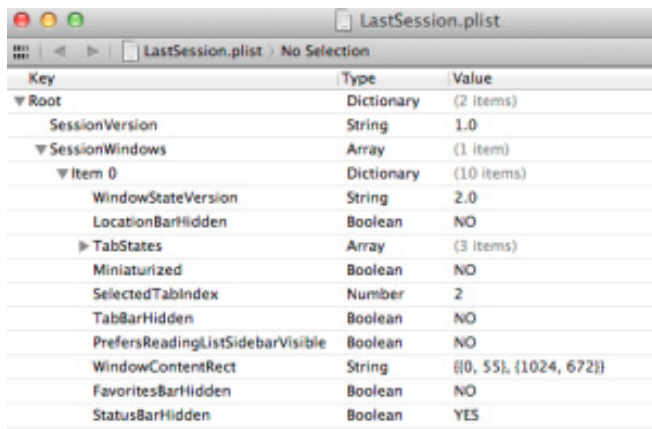


Figure 4. Browsing session ended unexpectedly

TabStates records the referred webpages in the present state. Each item in the TabStates is listed as a tab in Safari.

- TabTitle: records the title of the webpage
- TabURL: records the visited URL of the webpage

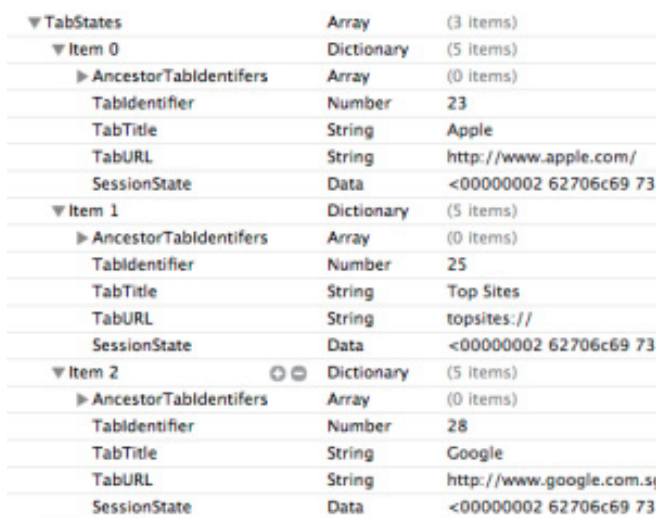


Figure 5. TabStates

## REFERENCES

- <http://zerosecurity.org/tutorials/safari-forensic-tutorial#>
- <http://forensicartifacts.com/2010/08/safari-browsing-history-mac/>
- <http://sci.tamucc.edu/~cams/projects/345.pdf>
- Jungsoon Oh, Seungbong Lee, Sangjin Lee, "Advanced evidence collection and analysis of web browser activity", digital investigation (2011), Science Direct, S62 – S70.
- [http://www.browserforensics.com/?page\\_id=50](http://www.browserforensics.com/?page_id=50)

## CACHE.DB

This file is located at ~/Library/Caches/com.apple.Safari. This is a SQLite 3 database and contains not only websites visited with corresponding timestamps but it also contains the images, scripts, etc. If the history is cleared, the information may still exist in cache. This database file will be resized when the user chooses to empty cache.

## IMPACT OF PRIVATE BROWSING

If the user turns on private browsing, the History.plist, LastSession.plist, and TopSites.plist files are not updated. Screenshots or previews of the websites will not be captured. You can attempt to carve for the webpages in unallocated space. If the Mac is still on, then a memory dump will provide a history of websites visited. You can use the terminal to review what is in memory or you can use some forensic tools to analyze live memory. Another method is to query the Cache.db file located at ~/Library/Caches/com.apple.Safari. Note that once the browser (operating in private mode) is closed, this file will be resized and the historical websites and embedded information cleared. If the browser crashes in the middle of private browsing, you can also look at crash logs for any web history that may be useful to your case.

## CONCLUSION

From the various examinations over Safari Browser, potential artifacts can be identified. That is very useful for browser based network forensics analysis. These artifacts are also useful for profiling the cybercrime and criminal psychology. List of artifacts can be varies in version to version. But almost artifacts remain default in each version. So, artifacts analysis related to safari browser can give lots of potential evidences.

# PTK Forensics professional

Collaborative  
Multi-tasking  
Easy-to-use  
Case and  
Evidence  
Management

## MAIN FEATURES

RAM  
Analysis

Registry  
Analysis

e-mail  
Analysis

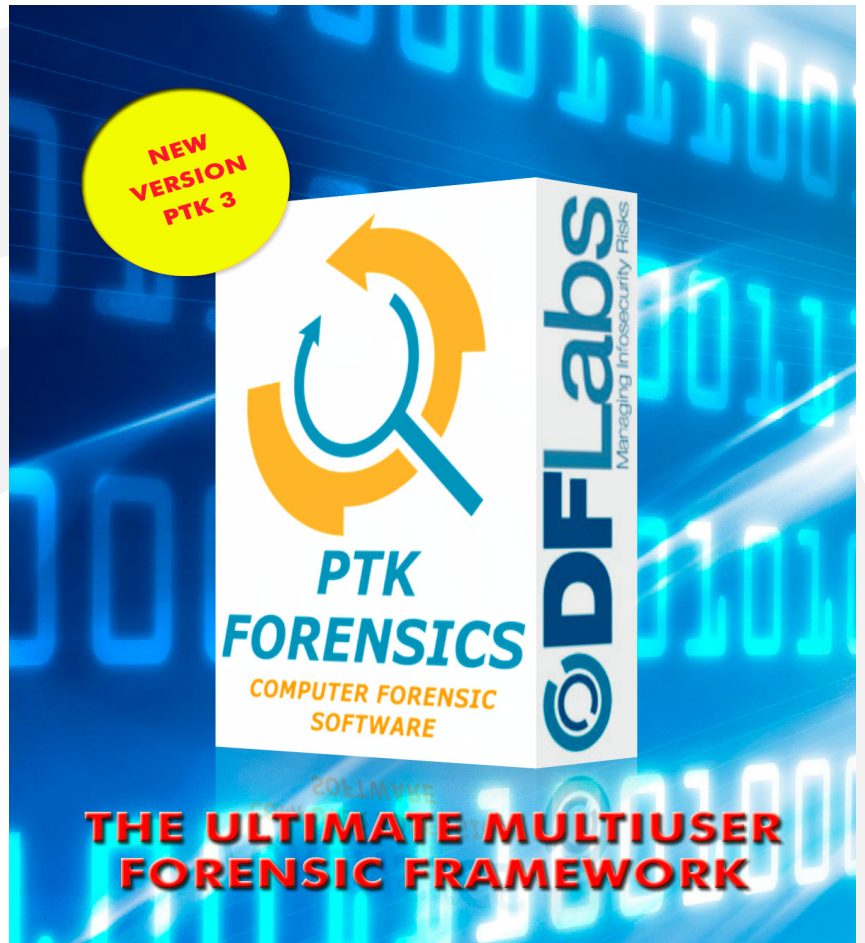
Timeline

Gallery

Keyword Search

Pre-Processing

Advanced  
Reporting  
System



**SPECIAL PROMO 15% OFF**  
single user perpetual license

<http://www.ptkforensic.com>

promo code **E-FORNCS13**

# BROWSER FORENSICS ON MACS: SAFARI!

by **John Reed** – Systems Administrator

What is browser forensics? Most folks probably have no idea what it is or why they need it. In a nutshell forensics will enable you to see what has been going on in your browser on your system or a browser on another system. What sites have been visited, how that system is being tracked, how often sites are seen and what content has been downloaded to that machine.

## What you will learn:

- How to discover browser data (history, cache, downloads) and analyze it
- How to discover internet/browser data even when users try to hide their tracks and how to disable them from doing so.
- How to monitor this content remotely.

## What you should know:

- General Understanding of Mac OS, and the Safari web browser
- How to download Xcode from the apple App Store
- General understanding of web concepts

In the last 10 years the Mac and it's siblings (iPhone, iPad) have made explosive growth in the enterprise market, from IT to sales and marketing. Macs have become present enough that sys admins have to pay attention to them and make sure that the Mac and it's users follow the rules, and subsequently be able to find out when they don't. Today we are going to talk forensics on the Macintosh platform, more specifically with its browser de-

jour, Safari. Ok so to delve into the inner workings of Safari on the Mac we need to start looking at 6 files, all of which are found in `~/Library/Safari/`

- Bookmarks.plist
- Cache.db
- Cookies.plist
- TopSites.plist
- History.plist
- LastSession.plist

These files are where the lion shed of information is stored for any and all activity inside Safari. You will note that all of these files are .plist or property lists. Mac OS X.x uses plists as a meta storage me-

dium for all kinds of systems and application related information, for all intensive purposes they are xml files. Before beginning your analyses of said files, you will want to download the Xcode tools from the App Store, they are free, provided by apple, and it includes a little app called plist editor that will make viewing and sifting through these files much easier.

All right now, let's take a look at one of the files... TopSites.plist. This particular file keeps a ranked record of what sites are most visited by the user who is browsing. The file contains the site title as well as the specific url of the site being visited. Also at the bottom of the file it shows when it was last updated to give you a better idea of when these popular sites were last visited. Take a look at the screen shot below to get an idea of what you will see: Figure 1.

This is a very telling file to look at even more so than the history.plist as it shows what sites are most frequently visited, not just the last ones visited. Another file that can also be pivotal to your forensic discovery, especially if the investigation time sensitive, is the LastSession.plist. This file lets you see what your user was viewing right up until they closed the application. It will allow you to get detailed levels of information, down to how many tabs they had open and what was being displayed on the those tabs, take a look: Figure 2.

You can browse through the other files listed here and gain a wealth of knowledge from the cookie data etc... to finding out what your users have been up to. The cache.db file is a bit of a different animal... It is actually a sqlite database that tracks/organizes the files that the browser caches, so this can give you some concrete (file based)



evidence for your investigation. Now one big gotcha in the forensics world when it comes to browsers is “private browsing” mode. This essentially nullifies any of the tracking and data you would be able to gather from the files I listed above, as they are never written to. But there is still hope! Many plug ins that are used in today’s browsers also keep a tidy little history for sites that have been browsed. Let’s take flash as an example: Any flash enabled website that is visited has its domain name recorded to `~/Library/Preferences/Macromedia/Flash Player/#SharedObjects/`, even with private browsing turned on! Another technique that can be used if a suspect user/machine is a little savvy and keeps their browser history and other files clean is to end run the browser entirely. Most modern switching equipment has the ability to clone the data coming from one port out to another port, you can then run a utility called tcpdump to collect all the network data being passed by that machine, this will in turn allow you collect the mac

address associated with all the network calls and log them off to a separate system for analysis. Also remember that at its core Mac OS is a UNIX based operating system and that almost anything can be scripted and run remotely, so making silent backups of the files I mentioned earlier, as well as other forms of analysis can be run silently and remotely. There are also commercially available purpose built programs specifically for forensic analysis and discovery, MacForensicsLab, DasBoot, Data Rescue and others... They are used and trusted by law enforcement and many others but also come with a heavy price tag. Hopefully this provides you with some insights to browser forensics on the mac platform and can help in your own investigations.

**ABOUT THE AUTHOR**

*John Reed has been a systems engineer for the past 16 years in a multitude of industries, specializing in Mac OS. E-Mail: Macguru80@gmail.com. Twitter: @MacGuru80*

Key	Type	Value
▼ Root	Dictionary	(3 items)
▶ BannedURLStrings	Array	(0 items)
▼ TopSites	Array	(12 items)
▼ Item 0	Dictionary	(2 items)
TopSiteURLString	String	http://www.newegg.com/
TopSiteTitle	String	Newegg.com – Computer Parts, Laptops, Electronics, and More!
▶ Item 1	Dictionary	(2 items)
▶ Item 2	Dictionary	(2 items)
▶ Item 3	Dictionary	(2 items)
▶ Item 4	Dictionary	(2 items)
▶ Item 5	Dictionary	(2 items)
▶ Item 6	Dictionary	(2 items)
TopSiteURLString	String	http://www.apple.com/
TopSiteTitle	String	Apple
▶ Item 7	Dictionary	(2 items)
▼ Item 8	Dictionary	(2 items)
TopSiteURLString	String	http://www.google.com/search?client=safari&rls=en&q=ubuntu+live+usb+for+mac&ie=UTF-8&oe=UTF-8
TopSiteTitle	String	ubuntu live usb for mac – Google Search
▶ Item 9	Dictionary	(2 items)
▼ Item 10	Dictionary	(2 items)
TopSiteURLString	String	http://www.peachpit.com/articles/article.aspx?p=1431816&seqNum=2
TopSiteTitle	String	Troubleshooting Binding Issues   Mac OS X Directory Services v10.6: Accessing an Active Directory Service   Peachpit
▶ Item 11	Dictionary	(2 items)
DisplayedSitesLastModified	Date	Sep 20, 2013 2:22:55 PM

Figure 1. TopSites.plist Example

Key	Type	Value
▼ Root	Dictionary	(2 items)
SessionVersion	String	1.0
▼ SessionWindows	Array	(1 item)
▼ Item 0	Dictionary	(10 items)
WindowStateVersion	String	2.0
LocationBarHidden	Boolean	NO
▼ TabStates	Array	(2 items)
▼ Item 0	Dictionary	(5 items)
AncestorTabIdentifiers	Array	(0 items)
TabIdentifier	Number	1
TabTitle	String	Reed-Dashboard – ClickBank Jira
TabURL	String	http://jira.clickbank.local:8082/jira/secure/Dashboard.jspa
SessionState	Data	<00000002 62706c69 73743030 d101025e 53657373 696f6e48 6973746f 7279d203 0405065f 101a5365 7373696f 6e486973 746f7279 43757272 656e7449 6e646578 5f101553 65>
▼ Item 1	Dictionary	(5 items)
AncestorTabIdentifiers	Array	(0 items)
TabIdentifier	Number	4
TabTitle	String	Slashdot (15)
TabURL	String	http://slashdot.org/?page=2
SessionState	Data	<00000002 62706c69 73743030 d101025e 53657373 696f6e48 6973746f 7279d203 0405065f 101a5365 7373696f 6e486973 746f7279 43757272 656e7449 6e646578 5f101553 65>
Miniaturized	Boolean	NO
SelectedTabIndex	Number	1
TabBarHidden	Boolean	NO
PrefsReadingListSidebarVisible	Boolean	NO
WindowContentRect	String	{{277, 165}, {1112, 842}}
FavoritesBarHidden	Boolean	NO
StatusBarHidden	Boolean	NO

Figure 2. LastSession.plist Example

# HOW TO AVOID SECURITY FLAWS IN APPS USING IOS WEB VIEWS

by Maria Davidenko

iOS is considered the most secure touch OS because of its closed nature. However, that doesn't mean that there is no place to worry about your data safety and integrity, or, to be more precise, about your user's data safety. There are plenty of tools developers get with the iOS SDK to provide a great user experience within their apps, there are, however, few tools you may use to provide safe Internet browsing within your apps. `UIWebView` is one of them.

## What you will learn:

- What are Web Views

## What you should know:

- Cross Site Scripting web view vulnerability
- How to protect your users from vulnerabilities
- Be familiar with Apple native UI concept

Of course, not every application would be attacked. And, of course, not every application, containing a `UIWebView` element as part of its GUI, would be attacked. Everything depends on the value of your data. Unfortunately, `UIWebView` is one of the most vulnerable elements in iOS. If at all possible – try and avoid its usage in your apps, to take care of your users. However, if you can't prevent its usage for any reason – beginning with customer requirements down to iOS limita-

tions in performing some tasks – you should be aware. We'll take a closer look at this iOS native object and discover how to protect your users while they browse web content.

## UIWEBVIEWS: WHAT ARE THOSE?

`UIWebView` is the native iOS element that lets you to embed web content in your applications. It is used to present various types of documents or HTML content. Let's give a few simple examples of `UIWebView` usage: Listing 1.

### Listing 1. Presenting web content in a `UIWebView`

```
NSURL *urlToPresent = [NSURL URLWithString:textField.text];
NSURLRequest *webRequestForWebview = [[NSURLRequest alloc]
initWithURL: urlToPresent];
self.webviewURLContent.delegate = self;
[self.webviewURLContent loadRequest:webRequestForWebview];
```

This small piece of code does one simple thing: it takes the content of a textfield (a URL) and displays the URL content to a user.

The next piece of code is used to present the content of some PDF documents, existing in the application sandbox (Listing 2). And the last small piece of code is used to present ANY content, received from a web server by your application: Listing 3.

These are classical examples of `UIWebView` class usage.

`UIWebView` may be considered as a lightweight Safari. It can render HTML, perform JavaScript scenarios – so it may be treated as a browser window – more or less.

`UIWebView` can also detect phone numbers, addresses, links and events for users to be able to interact with a web application content.

They help developers provide the users with great web content just within an app! Let's discover how safe they are.

## UIWEBVIEW AND SANDBOX

To remind you what a sandbox is, a Sandbox is a mechanism, intended to limit the application's access to the OS's internal data and to reduce the damage in a case, when a certain application has been attacked.

## FROM APPLE IOS APP PROGRAMMING GUIDE

"The purpose of a sandbox is to limit the damage that a compromised app can cause to the system. Sandboxes do not prevent attacks from happening to a particular app and it is still your responsibility to code defensively to prevent attacks."

Yes, the theory is sound. But what does it mean in practicality? In practice, iOS application sandbox is a structure of directories, each of which is intended to store the specific type of data. For example, Documents directory is intended to store the downloaded data or data created by the user within an app.

## FROM APPLE FILE SYSTEM PROGRAMMING GUIDE

"Use this directory to store critical user documents and app data files. Critical data is any data that cannot be recreated by your app, such as user-generated content."

`UIWebView` is able to parse and render data from HTML content. Potentially, users can download data to the Documents directory or any other directory of an application sandbox (This directory should be defined by a developer. Actually, Documents directory is used in 95% of all the cases of usage of the sandbox directories for storing the data). Doesn't sound good, does it? The malicious code downloaded by a user eventually may steal the data stored within your app's sandbox. For example, it may steal unencrypted list of sensitive data, e.g. credit card numbers.

Most of you reading these lines will say: "I never do it!" Or smile. Well, I'm glad if it brings a smile to your face. That means you're a person who takes care of their users.

There is an application sandbox, that protects the iOS from attacks by isolating an applications' data from any other data in iOS. `UIWebView` object allows developers to implement downloading the data to that sandbox, though this data may not be safe.

## NO CONTROL OVER WEB VIEW : THE MYTH AND REALITY

The one big problem with `UIWebView` is that developers almost have no control over it – this is Apple WebKit framework element. It is impossible to turn off most of its features – even if to turn it off is for users good. For example you cannot restrict the web view to load and execute the JavaScript code. But there are some features that you are able to control. You can limit or even deny loading of certain types of documents, supported by `UIWebView` which you consider as potentially dangerous.

### Listing 2. Presenting a PDF document with a `UIWebView`

```
NSString *documentName = @"some_document_name";
NSString *extantion = @"pdf";
NSString *path = [[NSBundle mainBundle] pathForResource:documentName ofType:extantion];
NSURL *url = [NSURL URLWithString:path];
NSURLRequest *request = [NSURLRequest requestWithURL:url];
[self.webviewURLContent loadRequest:request];
```

### Listing 3. Presenting a url, received from a web server in the JSON format

```
NSString *webViewURLString = parsedObjectFromWebServerJSONInput.url;
NSURLRequest *urlRequest = [[NSURLRequest alloc] initWithURL: [NSURL URLWithString:
webViewURLString]];
[self.webviewURLContent loadRequest: urlRequest];
```

## CAN PERFORM JAVASCRIPT

One more problem is that UIWebView can run JavaScript code. Javascript scenarios, which executed on a user's device is a potential danger for user's data. First of all it is dangerous because ANY JavaScript code may be executed.

## CROSS SITE SCRIPT VULNERABILITY IN UIWEBVIEW

Definition: "Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client side script into the Web pages viewed by other users." (Wikipedia)

In the context of a UIWebView XSS vulnerability may lead to sensitive user data theft. The following are the types of XSS vulnerability:

### PERSISTENT XSS

Definition: "The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping. A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read" (Wikipedia)

Consider the following scenario:

- UIWebView sends a request to load the URL.
- The malicious Javascript code has already been injected on the web server side
- The malicious code has been downloaded by UIWebView GUI element to an iOS user device and executed in the context of the application.
- For example, it can ask to enter a user's credentials data again, because of dropped connection.
- By entering his credentials data user sends it to attacker without even knowing about it.
- Just that simple. Well, it's not simple.

### NON PERSISTENT XSS

Definition: "The non-persistent (or reflected) cross-site scripting vulnerability is by far the most common type. [10] These holes show up when the data provided by a web client, most commonly in HTTP query parameters or in HTML form submissions, is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the request" (Wikipedia)

Non persistent XSS type of vulnerability could be exploited, for example, by sending users an e-mail, containing the malicious code within links that would be opened and executed by UIWebView. If a user uses native a Mail application as his e-mail client, links in e-mail messages would be opened

by default in Safari browser, UIWebView within an app is not involved in this process. However, consider the following scenario

- UIWebView send a request to load some URL.
- Attacker sends users an e-mail, looking "innocent" and "inviting" them to open malicious links.
- Users open the message within his e-mail app client (which is not Apple Mail), implementing its GUI via UIWebView and tap on any malicious link of the sent above.
- The link contains malicious JavaScript code
- The malicious code has been downloaded and executed by UIWebView GUI element within the application context.
- The attacker runs a javascript code on a iOS user's device, getting access to the sensitive user data.

An XSS vulnerability may occur in a poor written application that uses a UIWebView element as a part of its GUI. There are 2 types of XSS vulnerability: persistent and non persistent. Ultimately both of them acts by downloading some malicious code to a iOS user's device, which leads to sensitive user data theft.

## SOME SOLUTIONS

There are several techniques developer can use to protect users from a theft of their sensitive data. I shall speak of some of them. Of course, those are not the only techniques to protect your users and there are others, but they should be considered them next time you use a UIWebView object in your application GUI.

## USE QUICKLOOK FRAMEWORK TO PRESENT DOCUMENTS

Despite of the fact that `QLPreviewController` is a wrap around a UIWebView it is still more secure and right to use this class to present the document with your native apps. If you need more interaction with a document you may need `UIDocumentInteractionController`.

## VALIDATE YOUR REQUESTS BEFORE SENDING THEM TO UIWEBVIEW

As I said below, you cannot restrict the loading of JavaScript code within a web view, however you may do other thing. For example, you can restrict the loading of certain type of documents within your web view.

UIWebView has a handler for all requests in the web views within an app. A UIWebViewDelegate function `webView:shouldStartLoadWithRequest:navigationType:.` It returns a boolean value, indicating whether a web view will load content or not (Listing 4).

**Listing 4. Restricting UIWebView to load PDF documents**

```

- (void)viewDidLoad {

    NSString *pathToFileToLoad = [NSBundle.
mainBundle pathForResource:@"webview_security_
issues" ofType:@"pdf"];
    [self.webViewForTest
loadRequest:[NSURLRequest alloc]
initWithURL:[NSURL URLWithString:pathToFileTo
load]];
    [super viewDidLoad];
}
...
- (BOOL)webView:(UIWebView *)webView shouldS
tartLoadWithRequest:(NSURLRequest *)request
navigationType:(UIWebViewNavigationType)
navigationType {

    NSString *extantion = request.URL.
absoluteString.pathExtension;
    if ([[extantion uppercaseString]
isEqualToString:[PDF_EXTANTION
uppercaseString]]) {
        return NO;
    }

    return YES;
}

```

**Listing 5. Don't trust unknown certificates, avoid return YES in this delegate function**

```

- (BOOL)connection:(NSURLConnection *)
connection canAuthenticateAgainstProtectionSpa
ce:(NSURLProtectionSpace *)protectionSpace {
    return YES;
}

```

**Listing 6. Do not populate your obj-c variables values**

```

- (BOOL)webView:(UIWebView *)webView shouldS
tartLoadWithRequest:(NSURLRequest *)request
navigationType:(UIWebViewNavigationType)
navigationType {

    NSString *javaScriptString = [NSString
stringWithFormat:@"var username = \'%\'; var
password = \'%\''"];
    [someWebView stringByEvaluatingJavaScriptF
romString:javaScriptString];
    return YES;
}

```

**NEVER USE UNESCAPED DATA IN YOUR REQUESTS**

Do on your side everything to prevent the attack. Use escaped data only. Using escaped data reduces the risk of injecting the malicious JS code into your request.

**ENCRYPT THE SENSITIVE DATA STORED IN YOUR APP SANDBOX**

Well, it is not only related to a web views, but since the web views are vulnerable to XSS, it is highly recommended to encrypt your data.

**LET YOUR USERS TO DOWNLOAD THE DATA FROM TRUSTED RESOURCES ONLY**

Consider carefully the data downloading from the external web resource. It is not safe. However, if you have no other choice except of let users to download a data, ensure the resource has valid SSL certificate. One of a UIWebView flaws is that UIWebView let you load potentially untrusted web applications with ANY SSL certificate without prompting a user. Avoid this situation whenever it possible (Listing 5).

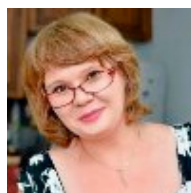
**NEVER POPULATE OBJECTIVE-C PARAMETERS VALUE TO JAVASCRIPT**

Never populate the values of Objective-C parameters. If the web application is vulnerable for XSS, the attacker may easily "steal" its values. Here is example what you SHOULD NOT do: Listing 6.

**IN SUMMARY**

Of course, there are more techniques, intended to protect the users against sensitive data theft, but those listed below should be taken into account first during the application creation process.

None of the written above doesn't mean, that you should panic each time the web view will appear in your apps. You need to consider carefully all the security aspects of your app instead. Knowing all the benefits and flaws of this object may be helpful in completing this task. Try to avoid UIWebView usage if you can by opening the links in the Safari browser and opening the documents in preview controllers. If you cannot avoid the UIWebView usage in your app – do everything on your side to protect the users.

**ABOUT THE AUTHOR**

*I've been working in different IT fields since 2005. The last 3 years I have been working in the iOS applications development field, developing network based applications. I've worked in the Oracle DB development field for 4.5 years, as well as in the integration field. A more complete profile can be found on LinkedIn <http://www.linkedin.com/in/mariyadavidenko>.*

# CYBERSECURITY IN ROMANIA

## A FIRST MAJOR ATTEMPT OF PUBLIC-PRIVATE COOPERATION & DIALOGUE PLATFORM IN ONE OF THE FASTEST-GROWING IT COUNTRIES

by **Laurent Chrzanovski**

Some may say it is another conference just to surf on one of the hottest issues of our times. Some may think too many NGOs are dealing with the same subject and sharing the same ambitions (for example *Cyber Crime Awareness Society*; *Cybervictims*; *Cybercrimeforum* etc). Probably both presumptions are right. And yet they do not fit the challenge we are trying to take on.

### What you will learn:

- What is the Police doing and what simple but fundamental advices can Intelligence Agencies and Police Forces give me to prevent a major part of the potential attacks against my company.
- What can I expect from the Law if my company has been harmed by hackers?
- How can I recover intentionally broken data and learn how the breach was possible?
- What can I do to make sure my employees do not leave my "IT-doors" opened?

### What you should know:

- Why Romania is one of the very best EU places to do IT and what does the Romanian State Institutions to counter cyber criminality.
- Which forms of economic crimes are being committed, from simple spams to intelligence hacking and how can they affect my life and my business.
- From the most "common sense" manual actions to the newest technologies, how can I prevent, fight and respond to a digital intrusion into my company's data.

As a matter of fact, Romania became one of the most interesting countries in the IT panorama of the very last years. According to several independent sources, the country is world-ranked 7th for the number of informatics specialists pro capite, 6th for the number of hackers, and 2nd after China for their dangerousness.

As a consequence, on the one hand, taking profit of so many highly qualified young specialists, several major IT companies (Google, Oracle, Microsoft, etc) established their regional headquarters in Bucharest, Cluj, Brasov or Timisoara, besides several big IT companies with Romanian capital. Romania is even the only country with USA and Russia that has a 100% Romanian-born and Romanian-managed global antivirus company, Bitdefender, which products are year after year classified among the very best ones in their categories.

On the other hand, national authorities are responding since a decade with an amazing dynamism to the threat constituted by Romanian hackers, who succeeded to rename the city of Râmnicu Valcea, now better known as "*Hackertown*".

A special, very proactive unit, the Service for Countering the Cyber Criminality, was created within the General Inspectorate of the Romanian Police, in collaboration with the Services for Countering Organized Criminality and Terrorism. This Service is now esteemed worldwide as one of the very best in Europe and was distinguished by many

awards for its collaboration in international operations coordinated by Europol and Interpol, not to mention the FBI.

The 23rd of May of this very year, the Parliament approved a National Cybernetic Security Strategy, where the CERT-RO (Romanian National Computer Security Incident Response Team) plays the central role of coordinating all the competent State departments from different ministries and services.

**ROMANIAN CONGRESSES PANORAMA AND THE URGENT NEED OF A DIALOGUE PLATFORM**

In this context, several conferences take place in Romania each year. They can be classified in three main types: the closed-doors ones, generally organized by the State Institutions, gathering the very best public and private specialists; the opened-doors yearly meetings dedicated to experts in the field, such as Defcamp or SecITC; finally, the one-day public speeches, most of them marketing-oriented.

Meanwhile, on the contrary to what happens in much less dynamic countries, there are no regular debate platforms between the three actors of the field: the State, the IT security solutions companies and the IT users, may them be from the public or

from the private sector, from the smallest one-man firms to the biggest companies.

If this year's very first edition will be successful, "Cybersecurity in Romania" ([www.cybersecurity-romania.ro](http://www.cybersecurity-romania.ro)) is designed to be a yearly neutral meeting point for a fruitful dialogue, which will also be enhanced by the presence of several international specialists from Italy, France, Switzerland and Norway. The conference priority is to be the most useful event for IT users to learn about all the new trends in cybercrime as well as all the new tools and methods to ensure a state-of-the art cyber-defense for companies and business.

**WHY COULD SWITZERLAND BE TAKEN AS AN EXAMPLE OF GOOD PRACTICES**

For achieving this challenge launched by the NGO Swiss Webacademy, based in Sibiu, the event will take place under the patronage and in presence of the Ambassador of Switzerland in Romania, H.E. Jean-Hubert Lebet. Three key-speakers trusted the initiative and will give their fundamental advises about how to concretize a real dialogue between the three parts: the World Coordinator for Cybersecurity at the International Telecommunication Union, M. Marco Obiso, the chairman of the EU forum for IPv6 implementation,

**LET US BUILD TOGETHER A SAFER IT WORLD IN ROMANIA!**

WHY NOT FOLLOW THE EXAMPLE OF THE OLDEST ROMANIAN CODE, NEVER HACKED IN MORE THAN 7000 YEARS?



One of the clay tablets found at Tartaria (Huedoara County, a hundred km. west from Sibiu), dated in laboratory ca. 5350 BC  
 Courtesy of the National Museum of History of Transylvania, Cluj-Napoca



Prof. Latif Ladid and, last but not least, the chief analyst of the Swiss Federal Intelligence Services, Mauro Vignati.

The last is one of the coordinators of MELANI, the Reporting and Analysis Centre for Information Assurance of the Swiss Confederation, where Police services, IT providers, IT companies and IT users, starting from entrepreneurial confederations, dialogue and share daily their problems, from the simple massive spams and “Nigerian mails” up to the most dangerous virus, trojans or targeted attacks.

The proposal met the interest of the highest responsables of the Romanian State, starting with the Presidential and the Prime-Minister advisors for Strategic National Security to the most important Ministries active in the field and, naturally, the Special Transmission Services from the Ministry of Defence and the CERT-RO. Two dozens of major IT security companies, professors from the most important national Universities and independent analysts also answered positively to the invitation to deliver a lecture, so now the real “*incognita*” will be how the IT users, i.e. the public, will interact with all the speakers.

Romania needs to back up all the efforts its Special Police forces and CERT with dialogue, consciousness raising and prevention among the IT users.

In an “evangelization” attempt, two renowned specialists of the Institute for Economic Crime Investigation (Neuchâtel) will introduce a thematic which is not so diffused in Romania, i.e. the human and the insider factor – from the simple mistakes to the intentional abuses – as a major source of security leaks in companies.

Our initiative is made in this sense, as a non-profit, non-marketing open space where speakers and participants will be able to speak together and learn each other’s problems, where every person has as much to learn as he/she has to share. All these experiences will be gathered and shared in a special volume of the academic journal *Studia Securitatis* of the ‘Lucian Blaga’ State University of Sibiu.

These concepts, and much more, will be discussed between specialists and users during the Conference “Cybersecurity in Romania. Challenges and Solutions for IT Security”, Sibiu, Hotel Ramada, 25-26 September, 2013.

Informations and inscriptions at: [www.cybersecurity-romania.ro](http://www.cybersecurity-romania.ro).

#### REFERENCES

- <http://www.bloomberg.com/slideshow/2013-04-23/top-ten-hacking-countries#slide5>
- According to a global IT IQ report made by Brainbench, Romanians already dominate Europe with more than 16,000 certified specialists;
- Verizon’s 2013 Data Breach Investigations report said 30 percent of 621 confirmed attacks were sourced back to China, 28 percent to Romania, and another 18 percent to the United States; Read more at: <http://phys.org/news/2013-04-china-romania-key-sources-hacking.html#jCp>
- UNODC, Comprehensive Study on Cybercrime, Draft – February 2013, p. 49; available at: [http://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf)
- Bhattacharjee, Y., 2011. Why Does A Remote Town In Romania Have So Many Cybercriminals? *Wired*, 19(2): 82
- Article from Le Monde, 01.07.2013, translated by Worldcrunch: <http://www.worldcrunch.com/tech-science/in-romania-a-quiet-city-has-become-the-global-hub-for-hackers-and-online-crooks/hacking-hacker-romania-pirate-scam-internet-website/c4s10532/#>
- In primis the prestigious ISEC award in 2011; see also: <http://www.scmagazine.com.au/News/347403,ranks-of-romanian-cyber-cops-surge.aspx>

For the Conference Organizers (Swiss Webacademy, Pfinder Consult, Asia, Agora & Mobile-Com) Dr. Laurent Chrzanovski.

#### ABOUT THE AUTHOR

*Priv.-Doz. Dr. Laurent CHRZANOVSKI is an Independent Archaeologist & Cultural Events Manager. He is also PR and International Relations Manager for the non-profit Professional Association Swiss Webacademy, Sibiu. With a PhD obtained at the University of Lausanne and a Postdoctoral Research Degree at the Romanian Academy of Sciences, Laurent CHRZANOVSKI is PhD Co-Director at the Lyon II Lumière University. He is also lecturer at the University of Sibiu and taught at the doctoral schools of the Universities of Fribourg, Lyon, Jerusalem and Stockholm; he is the author of 17 books and a hundred scientific articles, as well as of several international exhibitions. Linking the past with the future, he designed the UNESCO-ICOM 2011 exhibition prize winner “From the first writings to multimedia” and the special exhibition “Social media heroes, social media victims. From hieroglyphs to Facebook”, displayed at the ITU world headquarters (Geneva) in june-september 2013.*



web for your business  
swiss webacademy



P Finder Consult



Present:



# CYBERSECURITY IN ROMANIA

— conference —

Co-organizers:



# WEB BROWSER FORENSICS: Q&A WITH CCL-FORENSICS

by Indigo Larson

CCL was founded as an independent IT consultancy in 1986 by Andrew Krauze, the company's managing director, offering experienced and independent consultancy to ensure IT effectively supports business objectives. This forms the bedrock of CCL – our services and solutions are backed up by our team of highly knowledgeable consultants with years of industry experience behind them.



CCL (COMPUTER CONSULTANTS) LTD - Established 1986

CCL-FORENSICS LTD - Established 2001

CCL E-DISCLOSURE LTD - Established 2010

Over the years, CCL's offering has expanded, building on our digital forensics capability, to offer computer and mobile phone forensics, CCTV enhancement and cell site analysis, and expert witness services. CCL is now the UK's leading supplier of digital data investigation services.

Building on our IT consultancy heritage and expertise in digital forensics, CCL has broadened its offering to civil law firms and enterprises, providing solutions in data collections, investigations and e-disclosure. Key to CCL's success and longevity has been to maintain the flexibility to respond to market changes and, more importantly, the needs of businesses.

## What kind of information can be obtained from a web browser? Have you worked on any interesting cases recently?

There is a wealth of information that can be obtained from a web browser, this includes: web sites visited, search terms entered, saved form data, passwords, session recovery data, download information, social activity, communication, text and graphical captures of visited webpages (depending on the browser), etc. In a recent case we were asked to reconstruct a timeline of Internet activity in order to attempt to determine when a murder took place and if the crime was premeditated. In this case the artefacts recovered from the computer's Internet browser were able help provide an

insight into the user's state of mind and establish certain events leading up to the death.

### **How do your tools work with encrypted data?**

This depends on the nature of the encryption and how it is implemented. We use tools that are able to parse information from some encrypted sources, such as encrypted chat logs. If we are supplied with the key or password, then it is straightforward to decrypt. Or it might be a well understood encryption process such as ROT13.

There are various methods of decrypting data such as dictionary attacks, rainbow tables and brute-force attacks. You can also take advantage of the fact that people tend to use the same or similar passwords for different things. Some stored passwords are easier to locate. Therefore, these passwords can be used to attempt to decrypt other data that is identified.

### **How do you advise handling privacy settings on a browser i.e. IE8 automatic delete/overwrite the same history/cookie data file? In regards to using Dunk or epilog?**

In a historic case it was determined that the Internet history was purged at the end of each session on a public library computer that was used almost exclusively for Internet browsing on a single profile by multiple users. As the computer was seized after the next person following the suspect used the computer, recovering the deleted files meant also recovering files created by the user after the suspect. However, because of the way that computers work there was a strong possibility that these recovered files were written to the same clusters that had been used to hold the suspect's Internet activity files. Therefore, the slack space of the recovered files was examined and some Internet activity was identified which appeared to correspond with the sort of activity that the suspect might have undertaken; he was a drug trafficker. Not conclusive evidence, but the source of interesting intelligence on the suspect.

CCL-Forensics develops proprietary software tools to assist investigators with web browser/Internet evidence. For example, Dunk! analyses the cookie files which are placed on devices by web browsers, uncovering potential new evidence, as well as showing the path the user took to arrive at a particular webpage. epilog recovers and presents deleted data from SQLite databases. SQLite is so widely used that, without a tool like epilog, investigators could be missing out on crucial data without it. For example, in a recent case handled by CCL-Forensics, epilog recovered and presented nearly 5,000 entries from a smartphone's web cache, where there were only 400 live (visible) entries. For

more information on CCL-Forensics' software tools, please visit: [www.cclgrouppltd.com/software](http://www.cclgrouppltd.com/software).

### **In your experience, what are the most common mistakes made by First Responders? What advice would you give to potential First Responders?**

A common mistake is to examine the computer while it is running and thus potentially affecting the evidence. DO NOT HAVE A QUICK LOOK! Photograph the screen, note running processes and programs. Once you have an understanding of the situation, discuss the various options with the person in charge of the investigation. Always keep good contemporaneous notes of your actions.

### **What are the major challenges in e-disclosure?**

A traditional challenge in e-disclosure is that most review platforms do not handle none text-based sources well. This is due to the large size of multimedia files (and the associated cost), and the relatively small benefit in loading them into the review platform. Fortunately, at CCL-Forensics we have presented multimedia cases to the courts within our digital forensics cases since we established our laboratory in 2001. This has allowed us to devise methods for searching and presenting these files in the best way.

We are also seeing that regulators are becoming increasingly interested in reviewing the less formal methods of communication, such as voice communications and instant messaging. This has been highlighted in recent cases, such as the LIBOR investigation, where these non-standard communication channels are more likely to be used by individuals to ask for favours or break rules, rather than the more formal, traditional methods of communication like email. As such, this information is increasingly being brought into the scope of investigations. We have recently been looking at tools which have the ability to extract data from social media and webmail.

Another issue centres around what is legally allowed to be collected, e.g. data that is password protected. However, this is primarily an issue for lawyers and, as such, not something that CCL-Forensics provides advice on.

### **What is the most important guideline when working on a Criminal Defence case?**

Total and complete honesty. At the end of the day, the expert works for the court not the instructing solicitor and this applies equally to Prosecution cases.

**Thank you for your time.**



NATIONAL RETAIL CRIME CONFERENCE *Partnered with*

**RiskManager.ie**

Ireland's Security and Fire Website

## ***Welcome to The National Retail Crime Conference (NRCC) – Dublin 2013***

The National Retail Crime Conference (NRCC) is delighted to announce its inaugural event launching on the 16th October 2013 in the Citywest Conference Centre, Dublin. This conference will offer Retail/Loss Prevention and Security professionals the opportunity to come together for networking, information sharing and to gain intelligence on crime within the retail industry.

The aim of the conference is to bring you Education, First hand experiences, Awareness and Strategies to Prevent, Deter and Detect crime in your business. The speakers on the day will consist of professionals with 1<sup>st</sup> hand experience in Retail, Supply chains and E-crime.

This conference will give you access to the top Loss Prevention and Security Professionals in the industry, a unique opportunity you don't want to miss.

### **Speakers on the day include:**

- Dr Vivienne Mee, Rits Computer Forensic
- Inspector Niall Fetherstone, National Crime Prevention unit, An Garda Siochana
- Úna Dillon, Head of IPSO Card Services
- Assistant Commissioner Jack Nolan, Organisation of Development & Strategic Planning, An Garda Siochana
- Frank Gleeson, Retail Director, Topaz
- Tara Buckley, Director General, RGDATA
- John Mearls, Global Asset Protection, EBAY

### **Exhibitor Contact:**

Ann Daly +353 (0)1 6580389 or [ann@riskmanager.ie](mailto:ann@riskmanager.ie)  
*(Only a limited amount of stands available)*

### **Delegates Contact:**

Karen McNevin +353 (0)1 2910999 or [karen@nrcc.ie](mailto:karen@nrcc.ie)

***Please note: limited number of places available so book early to avoid disappointment***

 @tmforumorg #dd13

OCTOBER 28-31, 2013  
SAN JOSE, CALIFORNIA

# tmforum DIGITAL DISRUPTION 2013

CONQUER CHALLENGES. SEIZE OPPORTUNITIES.



READER SPECIAL  
15% off a gold pass  
simply use voucher code  
P5WCC5 when you register

## Crashing the party - digital services

Enabling businesses and enterprises to conquer challenges and seize opportunities presented by the digital world, Digital Disruption, TM Forum's all new, expanded event for the Americas, helps service providers and their partners address vital issues such as reducing cost and risk, improving market retention and growth and increasing revenue by introducing innovative new services. Engage with 150+ expert speakers over four days filled with critical insights, debate, TM Forum training, networking and hands-on opportunities that immerse you in exciting innovations and new ideas.

### Not your average conference...

#### • Four topic-driven Forums

- Agile Business and IT Forum
- Customer Engagement and Analytics Forum
- Delivering Enterprise Services Forum
- Disruptive Innovation Forum

#### • Innovation Zone:

Explore all things TM Forum; meet companies that are seizing the opportunities the digital world is creating:

- **Meet the experts**, learn about **TM Forum programs** and explore our award-winning series of **live Catalyst demos**, collaborative accelerator projects led by cutting edge service providers and suppliers
- Touch and feel some of the latest **disruptive technology** that is changing the way we live and work
- Watch live demos and learn more about **real digital services** that leverage the broad ecosystem
- Discover **innovative technology** from vendors showcasing their best products and services

#### • Networking

#### • TM Forum Training and MasterClasses

### For more information or to register now:

Email: [register@tmforum.org](mailto:register@tmforum.org) | Phone: +1 973 944 5100

Visit: [www.tmforum.org/dd13EF](http://www.tmforum.org/dd13EF)

### Keynotes include...



Daniel Sieberg  
*Head of Media Outreach  
& Official Spokesperson,  
Google*



Adrian Cockcroft  
*Director of Architecture,  
Cloud Systems, Netflix*



Georges Nahon  
*CEO, Orange*

Platinum Sponsor:

**NetCracker**<sup>®</sup>

# SECPOINT CLOUD PENETRATOR

by Casey Parman

Network security has rapidly become a significant part of Information Technology Infrastructure consisting of policies to prevent unauthorized access to data in a network. Without a strong security plan companies find themselves vulnerable to intrusion without any knowledge of a threat. The best solution is to hire a Security Specialist but this isn't always applicable; many companies can't afford to pay a specialist, or when they can, can they be sure their company is truly protected?

SecPoint introduces a service that will provide assistance monitoring network(s) of security risk that rapidly changes. To tell you the truth I'm always skeptical about the next great vulnerability scanner on the market. SecPoint once again lived up to their name; the Cloud Penetrator gives you an easy to use on demand vulnerability management system, and all that is needed is access to a web browser.

The Cloud Penetrator is one of a kind environment SecPoint created allowing customers to scan their network without any additional hardware or software. The web interface is very pleasant and has stress-free navigation. The Cloud Penetrator provides the ability to create specific scan templates, schedules, and standard vulnerability scans from anywhere that has internet access. The web interface also provides statistics, history, logs, and network tools (ping, whois, port scan, and mail server finder).

The Cloud Penetrator allows you to create scans multiple ways. Using a template allows you to receive email notifications when a new vulnerability

is found. Creating a schedule allows you to repeat scans (Daily, Weekly, Monthly, and Yearly). No matter how the scan is created the setup of how the system is analyzed is always the same. First, the scan should have a name that is easily distinguishable. This way you don't get lost after a few scans. After the scan is named you simply add the IP address or the CIDR. These are IP addresses that you're approved to scan, and already provided SecPoint with the appropriate agreement form. Finally, the type of scan will need to be chosen. This is where everything gets interesting. The Cloud Penetrator provides 7 default scans which can be further modified with advanced options. The default scans are Quick, Quick Web, Normal, OWSAP Top 10, Aggressive DoS, Extensive, and Extensive Firewall. Deciding which scan to run requires knowledge of what each scan does. Below each scan is listed and how it's actually performing the scan (Figure 1). For more information please visit: [http://www.secpoint.com/datasheet/Penetrator-Schematics\\_web.pdf](http://www.secpoint.com/datasheet/Penetrator-Schematics_web.pdf).

The information provided above will allow educated decisions to be made when deciding which



scan to use and when to use them. Always remember the more extensive scan will require more time. Once the type of scan has been chosen we can easily be done, but let's dive into the advanced setup options.

The Advanced setup enables each scan to be modified, allowing anyone to customize their scan to meet their specific needs. The advanced setup

allows you six options to configure notes, ports, dirs, vhost, email, and aggressive. Notes allow you to add a note to the scan, maybe the specific purpose of each scan. The ports option sets specific ports that the system will scan. Dirs allow single directories to be audited, targeting each attack only at that specific directory (Example: *www.mydomain.com/chickens*) you would only add "chickens". Vhost are

**SCAN TYPES:**

**QUICK SCAN**

Quick Scan over most common TCP-IP port numbers  
 -21, 22, 23, 25, 42, 43, 53, 67, 79, 80, 102, 110, 115, 119, 123, 135, 137, 143, 161, 179, 379,443, 445, 465, 636, 993, 995, 1026, 1080, 1090, 1433, 1521, 1677, 1701, 1720, 1723, 1900, 2409, 3101, 3306, 3389, 3390, 3535, 4321, 4664, 5190, 5500, 5631, 5632, 5900, 7070, 7100, 8000, 8080, 8799, 8880, 9100, 19430, 39720

**QUICK WEB SCAN ONLY**

Designed to be non-harmful and not flood the services by simulating humans' behavior

- Non harmful Scan with ports: 80,443, 8000, 8080, 8443
- Web Application Vulnerability Scanner WAS
- Web Crawler
- Google Hacking DB
- Joomla Security Scan
- Google Safe Browsing
- 50+ Blacklist Checks
- Wordpress Security Scan
- Windows, MAC, Linux, Nix, and other OS's

**NORMAL RECOMMENDED SCAN**

Designed to be non-harmful and not flood the services by simulating humans' behavior

- Scans 8000 among the most common ports
- Performs 55+ checks
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS, and much more.
- Everything Included in Quick Web Scan

**OWASP TOP 10 SCAN**

The OWASP Top 10 is a list of most common web application vulnerabilities.

More information: [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

- A1 – Injection
- A2 – Cross-Site Scripting (XSS)
- A3 – Broken Authentication and Sessions Management
- A4 – Insecure Direct object references
- A5 – Cross- Site Request Forgery (CSRF)
- A6 – Security Misconfiguration
- A7 – Insecure Cryptographic Storage
- A8 – Failure to Restrict URL Access
- A9 – Insufficient Transport Layer Protection
- A10 – Invalidated Redirects and Forwards

**AGGRESSIVE DOS SCAN**

- Designed to be a harmful scan
- Full Scan of all 65535 ports
- Overflow Attacks
- DoS Attacks
- Includes everything in Normal Scan

**EXTENSIVE SCAN – NON HARMFUL**

- Full Scan of all 65535 ports
- Includes everything in Normal Scan

**EXTENSIVE FIREWALL SCAN – NON HARMFUL**

- Same as Extensive Scan but designed for firewalls, because it tries to scan address that appears offline.

*\*Information above was obtained from within SecPoint Cloud Penetrator.*

Figure 1. Cloud Penetrator Scan types and description

Sel.	Date	Scan Name	profile	Status	H. M. L. I.	Options
<input type="checkbox"/>	2013-08-24	aggressive year..	Aggressive DoS ..	Completed	3 2 0 3	
<input type="checkbox"/>	2013-08-22	extensive	Extensive Firew..	Completed	3 2 0 3	
<input type="checkbox"/>	2013-08-19	Night Scan	OWASP Top 10 Sc..	Completed	3 2 0 3	
<input type="checkbox"/>	2013-08-03		Normal Recommen..	Completed	3 2 0 3	

Figure 2. Completed Scan Options

Compliance result: ⊗ Recommended Scan Not Compliant

Vulnerabilities: 8 potential vulnerabilities identified.

- High:3
- Medium:2
- Low:0
- Information:3

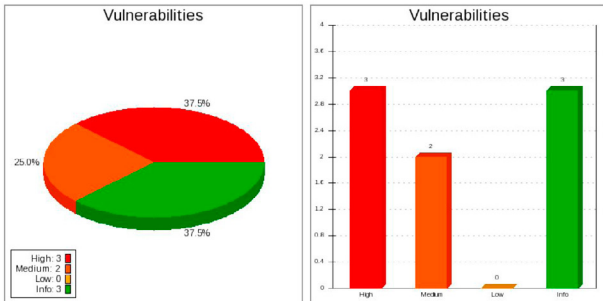


Figure 3. One Page Summary

used when several domain names run on the same IP address, and email simply notifies you when the scan has been completed. The aggressive are intended to be *harmful*, always remember that when you set them. They allow you to set the attack types of overflow, DoS, and bruteforce for any scan. With all of these options available any scan can be setup exactly as it's needed. Once the scan has been set-up the duration of the scan will depend on the op-

tions selected and the network it's scanning. Each scan preformed on my personal network took approximately 45 minutes. The process of setting up a scan from the web GUI was very user friendly, allowing you to fine tune the scan to exactly what is needed. I was very satisfied with the simplicity of setting up the audit, and I have confidence you will feel the similar experience.

This whole process of setting up the scan and waiting for it to finish would be pointless without valuable results. Once the scan is completed SecPoint allows you Many Options for viewing the report PDF, Web, One Page Summary, Full without Solution, and XML. With so many options these reports can be viewed on virtually any device (Figure 2). Within these options you also have the capability to recreate the PDF reports, repeat the scan, add false positives, archive, and delete the scan.

The Full report with solutions is the most informative report. It has 9 different sections packed with information about the audit. The first two sections are the Introduction and the Vulnerability Details. These sections of the report are fully informative on how the rest of the report is laid out. The first part of the report that is exclusive for the particular audit is the Executive Summary. This is a

### Ports ad Service for IP:

Port	Protocol	Status	Service
463	tcp	open	alpes
862	tcp	open	Two-way Active Measurement Protocol (TWAMP) Control
1723	tcp	open	pptp

Figure 4. Ports are services results

### Service Version Banner for IP:

Banner name	SSHd Version Banner
Port	862/tcp
Details	SSH-2.0-OpenSSH_5.4p1 FreeBSD-20100308

Figure 5. Services Version Banner outputs

Vulnerability	Point-To-Point (PPTP) Protocol tcp port 1723 identified
Risk Level	Medium
SecPoint ID	53
BugtraqID	<a href="#">2111</a>
BugtraqID	<a href="#">2549</a>
BugtraqID	<a href="#">3022</a>
BugtraqID	<a href="#">2549</a>
BugtraqID	<a href="#">7582</a>
BugtraqID	<a href="#">7590</a>
Impact	Several services running the identified port is subject to many vulnerabilities specially Denial of Service attacks.

Figure 6. Vulnerability Identification output



quick overview of the scan results, made for management personnel. The last six section of the report are very informative, presenting the results of the audit more in-depth for IT professionals. Traceroute, Ports and Services, Banner Identification, Summary of Vulnerabilities, Vulnerabilities, and Gap Analysis. This report has everything you need to really analyze any network. Each section has valuable information; the traceroute section correctly verified that my network was blocking ICMP traffic. While the Ports and Services section shows what the ports services are commonly tied to, not what service is actually using them (Figure 4).

This could be looked at as a bad thing, but in reality this is exactly what a penetration tester will be looking at until they get more information. Where do they get that information, well SecPoint included it in the results too Banner Identification, it shows any banner information provided by the actually service running on the system (Figure 5).

As you can see I'm truly not running Two-way Active Measurement Protocol Control on port 862. Also you might have noticed that I have not added any solutions with my images. I figured it would be best if I kept them out so you can discover them for yourselves.

The next two sections are dedicated to the vulnerabilities found during the audit. The summary gives a brief description of each risk category and the treats found. While the Vulnerabilities a section provides further details into each threat. Surprisingly the only High risk vulnerabilities found during the audit was three different blacklists. I say surprisingly because I did not expect to see a blacklist listed as vulnerabilities but I defiantly understand the impact it can have for any business. Provided with each vulnerability assessment provided is the risk level, SecPoint ID, Impact, and Solution. The SecPoint ID is the official SecPoint ID of the vulnerability. For more information on each vulnerability please visit <http://www.secpoint.com/libpage.php> If applicable SecPoint also provides you with BugtraqID, CVE, and USN information that you

can easily click the number to verify the existence of the discovered vulnerabilities (Figure 6).

The final section of the report is the Gap Analysis which will show you what has changed since the last audit. This section can be very important when wanting to know the differences between scans without having to investigate each section. Besides the Full report the 1 page summary is a good report to give to management. Showing the number discoveries found during the audit in an easy to read report.

Scan statistics is another great feature SecPoint provides, but be warned that you need to enable global logging, global logging saves sensitive information associated with your IP to the system. If you do not wish to have your sensitive information saved you need to turn global logging off. Statistics shows the information obtained by each audit. As you can see my results never changed since I have not made any modification to my network (Figure 7).

SecPoint Cloud Penetrator is a great service, any great service can constantly be improved. I was only disappointed with the results of my aggressive scan, which took advantage of overflow, DoS, and bruteforce attacks. Setting up the scan worked as I expected, but once I got the report I realized that no information was provided about the success or failure of any of the attacks. I think SecPoint should provide this information to make their service truly irreplaceable. As a convenience it would be more practical for SecPoint to provide links to their SecPoint ID like they do for Bugtraq ID's. The only other section I felt could be improved was the information provided with in the blacklist results. I felt like I was reading the same information for each discovery except no information was truly provide on how to resolve the issue. Overall each person will have their own experience. I challenge you to try this service for yourself for free at: <http://www.secpoint.com/free-vulnerability-scan.php>.

There are two approaches to security, proactive and active. May organizations only rely on active measures (Only fix something once it's actually broken). SecPoint Cloud Penetrator gives you a proactive approach allowing you to resolve insecure areas of your network before it's too late. I was impressed with functionality and quality of the service SecPoint is providing. I would recommend this service to anyone looking for a reliable way to audit their network. With SecPoint Cloud Penetrator you no longer have to have the "we're safe, until it's too late" approach leaving your network infrastructure and private data secure.

Purchasing and more information can be found at <http://www.secpoint.com/cloud-penetrator.html>.

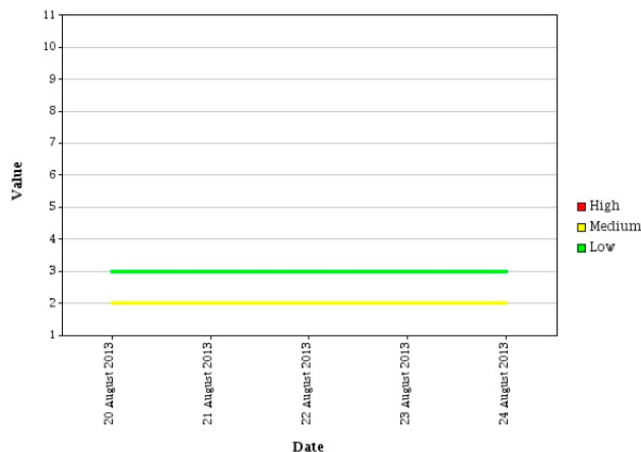


Figure 7. Scan Statistics Graph

# LAWTECH EUROPE CONGRESS COLLABORATES WITH LEADING TECHNOLOGY PROVIDERS CISCO AND ALUCID FOR EFFICIENT VIDEO STREAMING AND SECURE AUTHENTICATION

## by LawTech Europe Congress Collaborates

For the first time, LTEC participants can attend its annual event via live streaming video with the support of Cisco TelePresence®. In addition, all LTEC delegates will be provided secure authentication keys compliments of ALUCID®. LTEC is Central & Eastern Europe's preeminent event on electronic evidence, forensic investigations, cyber security, and legal technology.

Prague, Czech Republic (PRWEB UK) 30 September 2013

LawTech Europe Congress, the annual event on electronic evidence, forensic investigations, cyber security, and legal technology, is very pleased to announce its collaboration with two world class technology giants, Cisco and ALUCID. Their invaluable technology will surely make LTEC2013 a more accessible and security-minded conference.

With the power of Cisco TelePresence® SX20 Quick Set (SX20 Quick Set), LTEC2013 will be available via live streaming video. This will allow participants who are unable to attend the conference in person, the opportunity to attend from anywhere in the world. To attend the conference via live streaming, [click here](#).

*"LTEC is very privileged to be collaborating with Cisco and ALUCID. With their extensive ability to deliver cutting-edge technologies, we feel very strongly that the participants of LawTech Europe Congress 2013 will equally benefit from this collaboration."*

With ALUCID technology, LTEC 2013 delegates will have access to all the exclusive congress materials enjoying authentication which is highly secure yet very convenient, consisting of one-click operations and intuitive actions without passwords.

Electronic Evidence

Computer Forensics

Cyber Security

Legal Technology

21 - 22 October, 2013

Clarion Congress  
Hotel Prague

Register on

[www.lawtecheuropecongress.com](http://www.lawtecheuropecongress.com)



Frederick Gyebi-Ababio, Executive Director of E-Discovery Europe and founder of LawTech Europe Congress says of the collaboration: "LTEC is very privileged to be collaborating with Cisco and ALUCID. With their extensive ability to deliver cutting-edge technologies, we feel very strongly that the participants of LawTech Europe Congress 2013 will equally benefit from this collaboration."

**About ALUCID:**

ALUCID is an electronic identity repository representing real users in cyberspace. An individual user can be represented by various electronic identities that can be used in miscellaneous applications, such as online shopping, Internet banking or accessing e-mail accounts. The user no longer needs to remember dozens of different logins and passwords securing his/her various Internet accounts. With ALUCID®, randomly generated keys are used for authentication, not user's personal data (such as his/her e-mail or password).



**About LawTech Europe Congress:**

LawTech Europe Congress' mission is to create a cutting edge legal technology educational forum that address four core areas, e-discovery, forensics, cyber security, and legal technology. These disciplines are at the forefront within organizations globally and LTEC's guiding philosophy is to embrace solutions to empower law firms, corporations, and government institutions to reduce risk, limit the potential for expensive legal exposure and to increase overall competence around these topics. Delegates will be engaged throughout our events with advanced topic presentations, panel discussion, and practical demonstrations of the latest solutions. This event strategically focuses on best practices and how they fit into upholding a high level educational structure. LawTech Europe Congress has set out to provide relevant solutions and advice to all professionals interested in the future of digital evidence, forensics, cyber security, and law office technologies.

# Big Data gets real at Big Data TechCon!

Discover how to master Big Data from real-world practitioners – instructors who work in the trenches and can teach you from real-world experience!

## Come to Big Data TechCon to learn the best ways to:

- Collect, sort and store massive quantities of structured and unstructured data
- Process real-time data pouring into your organization
- Master Big Data tools and technologies like Hadoop, Map/Reduce, NoSQL databases, and more

Over 60  
how-to  
practical classes  
and tutorials  
to choose  
from!

- Learn HOW TO integrate data-collection technologies with analysis and business-analysis tools to produce the kind of workable information and reports your organization needs
- Understand HOW TO leverage Big Data to help your organization today

**“Big Data TechCon is loaded with great networking opportunities and has a good mix of classes with technical depth, as well as overviews. It’s a good, technically-focused conference for developers.”**

—Kim Palko, Principal Product Manager, Red Hat

**“Big Data TechCon is great for beginners as well as advanced Big Data practitioners. It’s a great conference!”**

—Ryan Wood, Software Systems Analyst, Government of Canada

**“If you’re in or about to get into Big Data, this is the conference to go to.”**

—Jimmy Chung, Manager, Reports Development, Avectra

# BigData TECHCON

## San Francisco

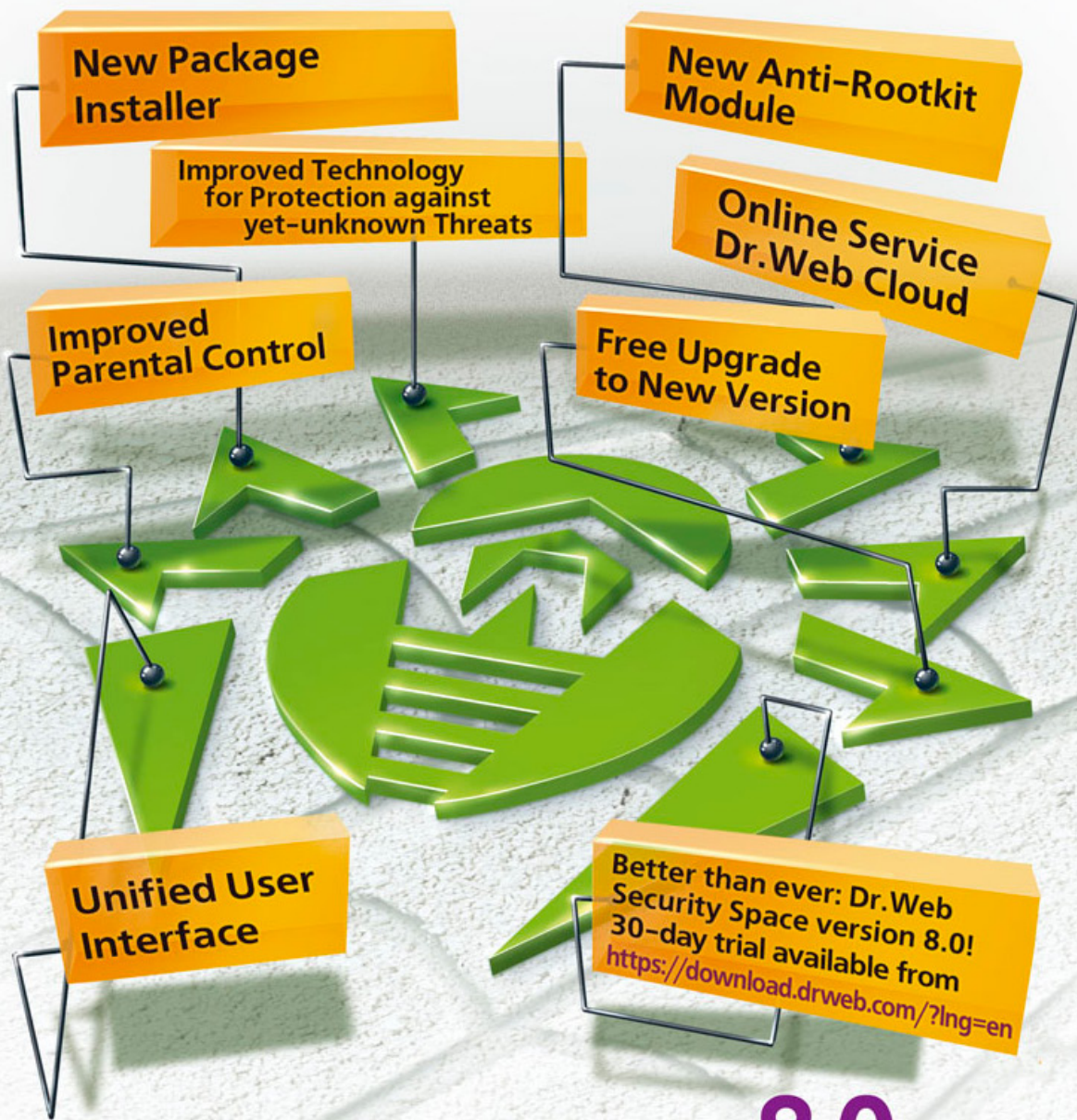
### October 15-17, 2013

[www.BigDataTechCon.com](http://www.BigDataTechCon.com)

The **HOW-TO** conference for Big Data and IT professionals



# Dr.Web SpIDer is 8-legged!



## New Version 8.0

### Security Space and Dr.Web Antivirus for Windows

Get your free 60-day license under <https://www.drweb.com/press/> to protect your PC and your smartphone with Dr.Web!

Your promo code: **Hakin9**

**Protect your mobile device free of charge!**

[https://support.drweb.com/free\\_mobile/](https://support.drweb.com/free_mobile/)



UPDATE  
NOW WITH  
**STIG**  
AUDITING

“ IN SOME CASES  
**nipper studio**  
HAS VIRTUALLY  
**REMOVED**  
the **NEED FOR** a  
**MANUAL AUDIT** ”  
CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at [www.titania.com](http://www.titania.com)



[www.titania.com](http://www.titania.com)