

Browser Forensics

Collecting evidence from today's
web browsers

Justin Hall & Nate Hausrath




Lots of things are browsers



“A web browser?
In *my* car?”

It's more likely than you think.

FREE PC CHECK!

 CONTENTwatch™



Even cars

What kind of evidence can we get?

Timeline of activity

Sites visited

Searches

Files transferred

Credentials used

Where is it stored?

History*

Search Activity*

Cache

Bookmarks

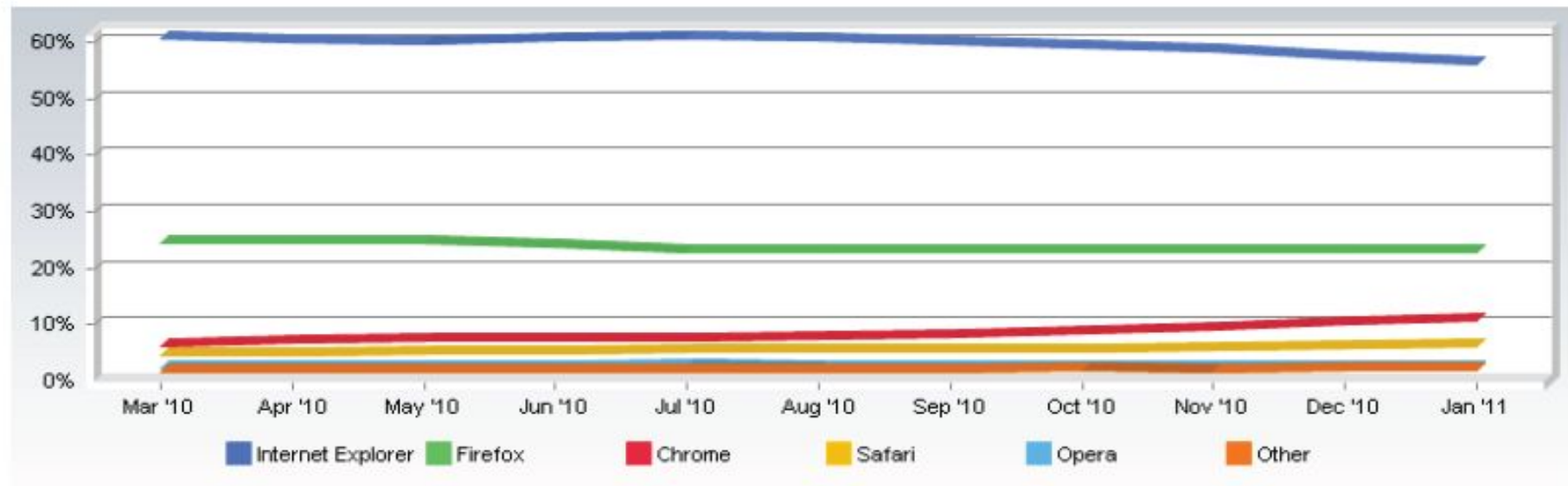
Stored Form Data

Stored Credentials

Cookies

Top Browser Share Trend

March, 2010 to January, 2011



Month	Internet Explorer	Firefox	Chrome	Safari	Opera	Other
March, 2010	60.65%	24.52%	6.13%	4.65%	2.37%	1.67%
April, 2010	59.95%	24.59%	6.73%	4.72%	2.30%	1.71%
May, 2010	59.75%	24.32%	7.04%	4.77%	2.43%	1.69%
June, 2010	60.32%	23.81%	7.24%	4.85%	2.27%	1.51%
July, 2010	60.74%	22.91%	7.16%	5.09%	2.45%	1.66%
August, 2010	60.48%	22.90%	7.50%	5.15%	2.36%	1.61%
September, 2010	59.62%	22.97%	7.99%	5.27%	2.40%	1.75%
October, 2010	59.18%	22.83%	8.50%	5.36%	2.29%	1.85%
November, 2010	58.44%	22.76%	9.26%	5.55%	2.20%	1.79%
December, 2010	57.08%	22.81%	9.98%	5.89%	2.23%	2.01%
January, 2011	56.00%	22.75%	10.70%	6.30%	2.28%	1.98%

Who's winning the browser wars?

Internet Explorer 8

Uses registry and filesystem

Disparity with different Windows versions

Not all index.dat files are alike!

Critical tools



Mozilla Firefox 3

Multiplatform, open source

Uses SQLITE3 DB for majority of stored data

Can be run self-contained on removable media

Critical tools



Google Chrome 9

Multiplatform

Built on open-source Chromium project

Uses SQLITE3 DB for majority of stored data

Critical tools



Apple Safari 5

"Multiplatform"

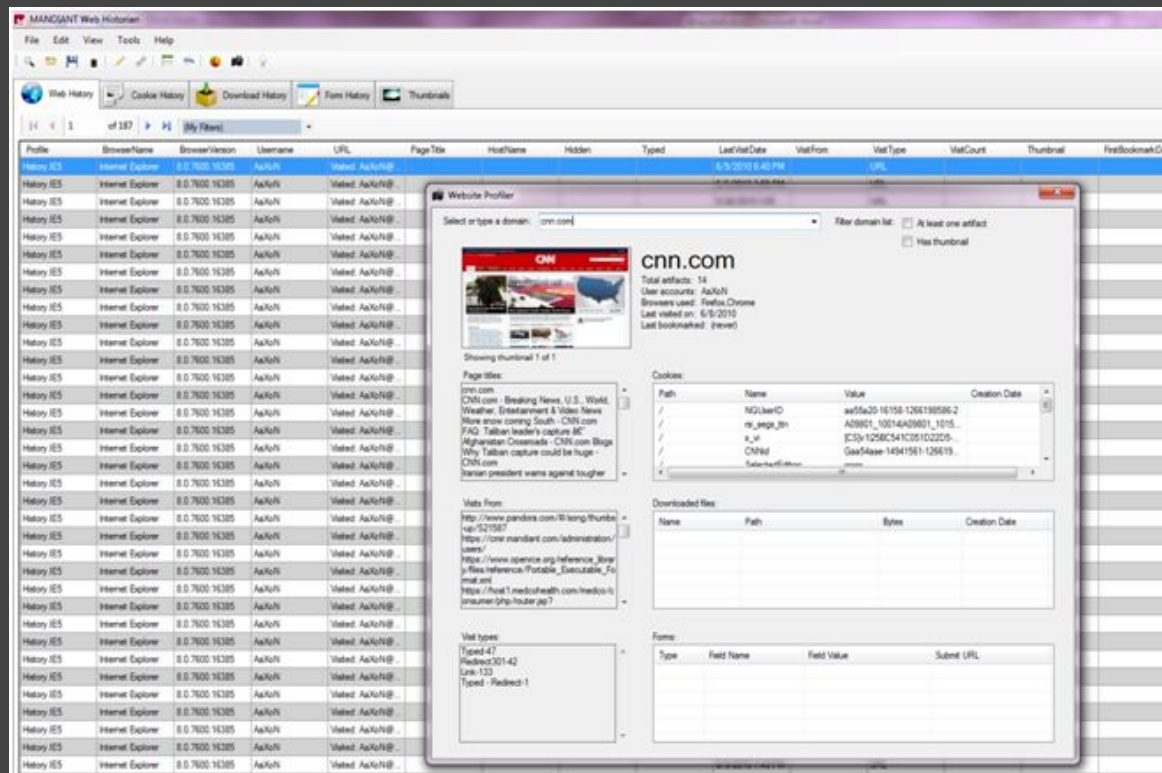
Stores data in Apple Property List files
and SQLite databases
Is made by f!@#\$ Apple



Critical tools

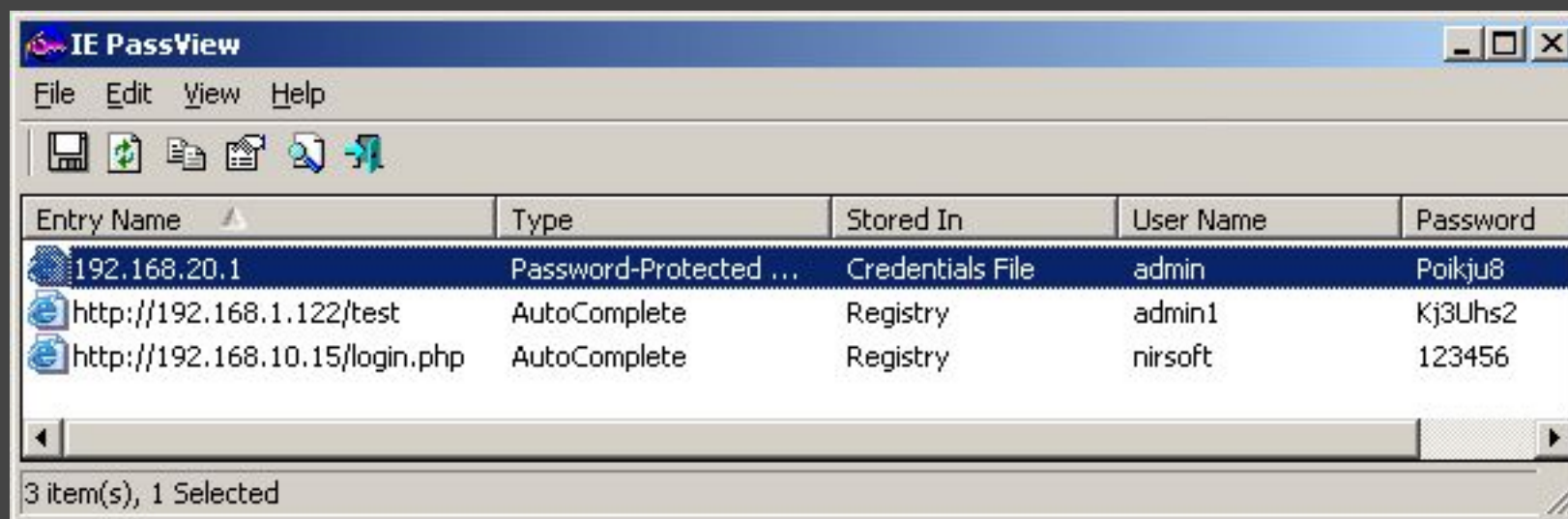


Free to download from
mandiant.com



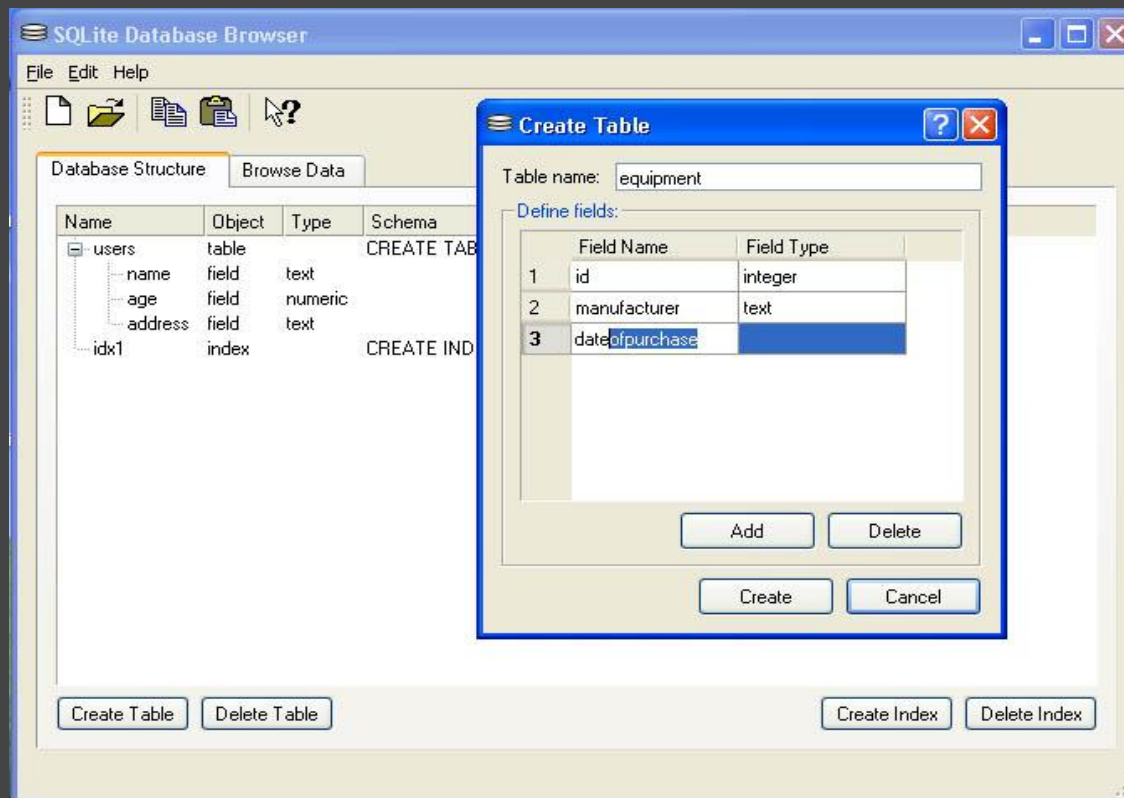
Nirsoft IEPassView

Free to download from
nirsoft.net



SQLite Browser

Free to download from
sqlitebrowser.sf.net





Questions?