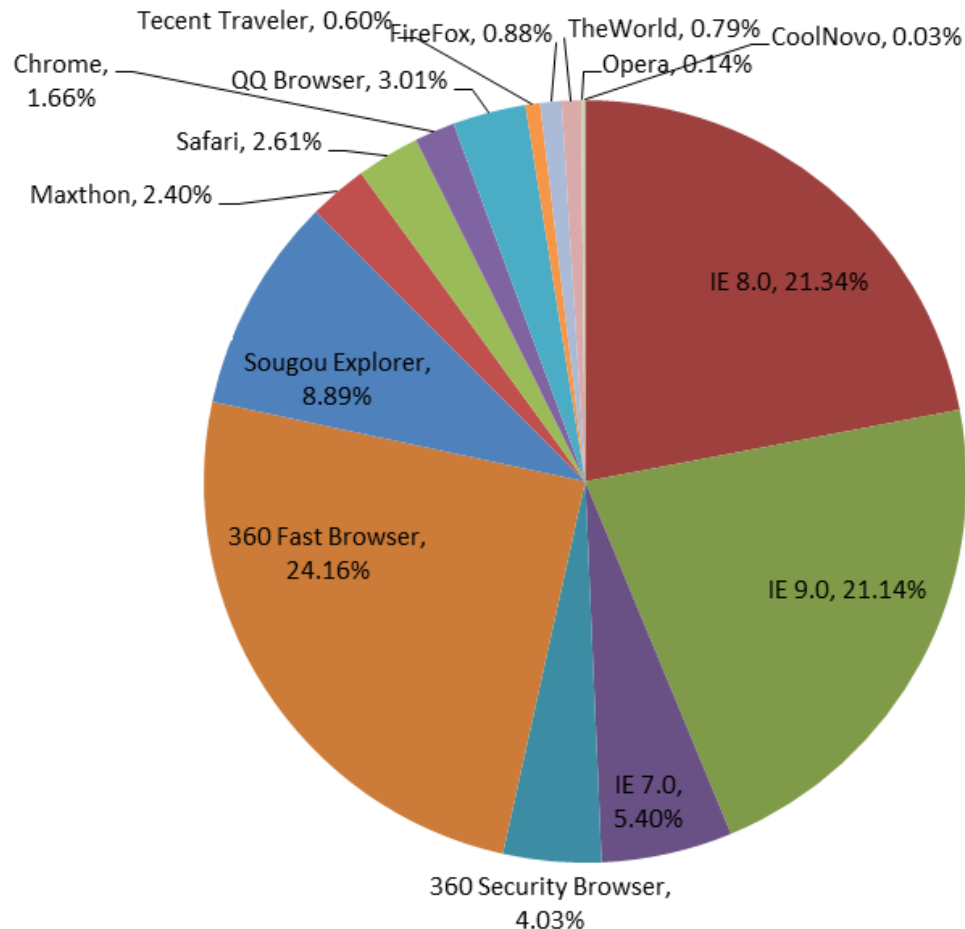


Forensic Analysis of Web Browser with Dual Layout Engine

Linda Zhong

Market share of Web browsers in China



Web Browser Type	Market share
Internet Explorer	51.91%
` Internet Explorer 6.0	21.34%
` Internet Explorer 8.0	21.14%
` Internet Explorer 9.0	5.40%
` Internet Explorer 7.0	4.03%
360	27.10%
` 360 Security Brower	24.16%
` 360 Fast Brower	2.94%
<u>Sougou Explorer</u>	8.89%
<u>Maxthon</u>	2.40%
Safari	2.61%
Chrome	1.66%
<u>Tencent</u>	3.61%
` QQ Browser	3.01%
` Traveler	0.60%
Firefox	0.88%
<u>TheWorld</u>	0.79%
Opera	0.14%
<u>CoolNovo</u>	0.03%

Chinese Web Browsers

- Maxthon 2
- Tencent Traveler(updated to version 6 with the new name QQ Browser)
- TheWorld
- 360 Security Browser

They all used IE Trident engine, i.e. all log files left are IE artifacts which can be analyzed by every web browser forensics tools

Recent Chinese Web Browsers

- Use the new layout engine
- Most of them have two access modes:
 - Fast mode: bases on IE Trident engine
 - Compatibility mode: uses WebKit or Chromium engine (Webkit also used by iOS and Android)



Recent Chinese Web Browsers

● QQ Browser, Maxthon 3 and Sougou Explorer use the IE and WebKit engines

● 360 Chrome and CoolNovo are based on the IE and Chromium engines

- Artifacts left by IE engine can be collected by forensic tools
- How about the artifacts generated by Webkit?

Why dual engine?

- Some web sites in China must be accessed by installing security plug-ins or add-ons, especially for banks and governments
- Plug-in or add-ons only support IE



**What can we do in
forensics analysis?**

Collection – Where to collect

○XP :

- C:\Documents and Settings\[User]\ApplicationData\[Application name]
- C:\Documents and Settings \ [User] \Local Settings\Application Data\[Application name]
- Installed path

○Vista/7:

●Webkit:

C: \ [User] \AppData\Roaming\[Application Name]

●Chromium:

C: \ [User] \AppData\Local\[Application Name]

●**Don't Forget to collect IE artifacts**

Collection – What to collect?

- Favorite
- Cookies
- History
- Download lists
- More
- Most of log files are in sqlite3 format

Analysis – Timeline Analysis

- 3 types of time stamps:

- Readable time format

- 2012-01-01 00:00:00(history records of Sougou Explorer)

- Webkit time format

- microseconds (10-6) since January 1 1601 00:00:00(UTC)

- UNIX time format

- seconds since January 1, 1970
00:00:00(UTC)

- Don't forget the time zone

Readable timestamp - Sougou Explorer history records

SQLite Database Browser - C:\Users\Linda\AppData\Roaming\SogouExplorer\HistoryUrl.db

File Edit View Help

Database Structure Browse Data Execute SQL

Table: UndoUrl

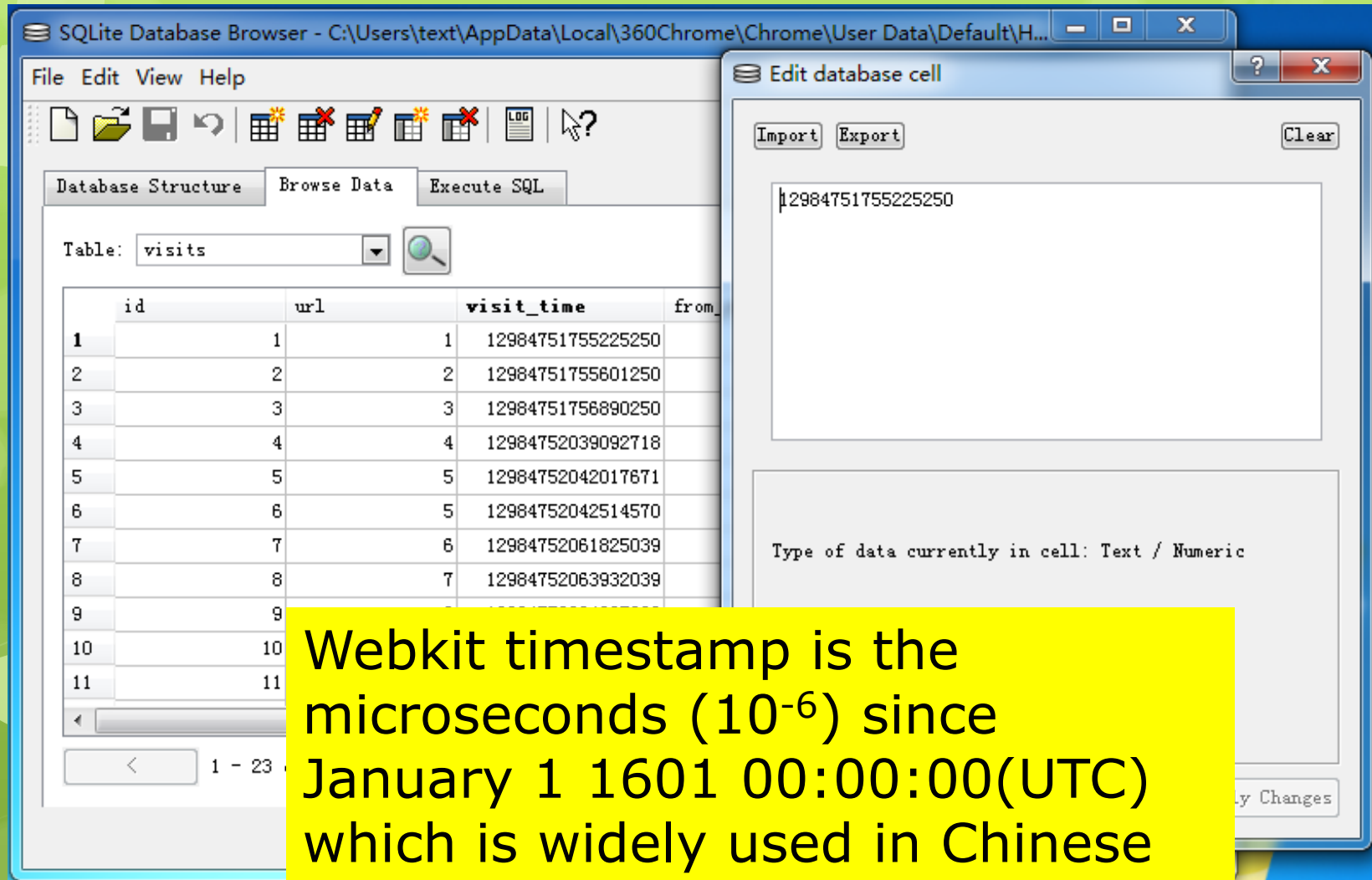
New Record Delete Record

	id	title	last
1	http://tv.tudou.com/	电视剧频道 视频_播客_个人多媒体	2012-06-22 15:34:00
2	http://www.tudou.com/albumplay/UXMXu_YGUNQ/FS	幽灵_在线观看8个视频_土豆网_剧	2012-06-22 15:34:00
3	http://dict.bing.com.cn/#%E4%BB%A5...%E4%B8%B	必应词典 (Beta), 在线词典, 在线翻	2012-06-22 15:34:00
4	http://www.baidu.com/s?bs=sqlite+format&f=8&r	百度搜索_sqlite format blob	2012-06-22 15:34:00
5	http://blog.csdn.net/aasmfox/article/details/	SQLITE3 读写二进制字段blob - 大	2012-06-22 15:34:00
6	http://zhidao.baidu.com/question/376255289.ht	SQLite format 3文件如何转成可读	2012-06-22 15:34:00
7	http://www.baidu.com/s?tn=sogouie_dg&bs=%CB%D	百度搜索_sqlite database browse	2012-06-22 15:34:00

< 1 - 7 of 7 >

Go to: 0

Webkit Timestamp



The screenshot shows the SQLite Database Browser application. The main window displays a table named 'visits' with the following columns: id, url, visit_time, and from. The table contains 11 rows of data. An 'Edit database cell' dialog box is open, showing the value '12984751755225250' in a text field. Below the text field, it says 'Type of data currently in cell: Text / Numeric'. The dialog box also has 'Import', 'Export', and 'Clear' buttons.

	id	url	visit_time	from
1	1		12984751755225250	
2	2		12984751755601250	
3	3		12984751756890250	
4	4		12984752039092718	
5	5		12984752042017671	
6	6		12984752042514570	
7	7		12984752061825039	
8	8		12984752063932039	
9	9			
10	10			
11	11			

Webkit timestamp is the microseconds (10^{-6}) since January 1 1601 00:00:00(UTC) which is widely used in Chinese Web Browsers

Analysis - Finding Searching Words

- Why? Search words are evidence of the suspect's efforts to gather information for his crime and may specify the purpose, target and methods of the crime
- Log file - 360 Chrome and CoolNovo/ChromePlus
- History file - HTTP URL structure

http://	Host	Port	/	Path	?	Search part(Variable= Value)*
---------	------	------	---	------	---	-------------------------------

For example:

- Baidu search:
- Host = Baidu.com
- Path=s
- Variable=wd

Analysis – Data Recovery

- 3 ways to delete data in sqlite3 files
 - Overwritten with zeros **Difficult to recover**
 - To delete the area itself
 - To set the data area as free
- Other formats usually deleted themselves
 - Possible to recover
- **These web browsers support function that auto-erase after every exit**

Deleting log files of Chinese web browsers

Web browser	History	Cookies	Cache(Folder)	Download list
Sougou Explorer	Overwriting by zero	Overwriting by zero	Deleted	Overwriting by zero
Maxthon 3	Overwriting by zero	N/A	Deleted	Deleted
QQ Browser	Overwriting by zero	Overwriting by zero	Deleted	deleted
360 Chrome	Overwriting by zero	Overwriting by zero	Deleted	Overwriting by zero
CoolNovo/ChromePlus	Overwriting by zero	Overwriting by zero	Deleted	Overwriting by zero

Analysis – Useful Logs

- My Favorite Sites/Most Accessed Sites
- Recently Closed Sites
 - Contain more time attributes
 - Both can be deleted with function auto-erase
- Special logs
 - contain forensic-sensitive information but can't be deleted by erase function.
 - based on understanding the structures of all the logs.
 - but not every browser has special logs
 - For example, **backups and crash logs**

Where are they?

Web browser	My favorite web sites	Recently closed pages	Favorite
Sougou Explorer	HistoryUrl.db	HistoryUrl.db	Favorite2.dat
Maxthon 3	-	Lasttab.dat	Favorite.dat
QQ Browser	{ED81EB6C-3DC4-4322-96F1-1B8716C404C4}.db	recent_closed_tab.db	Bookmarks
360 Chrome	Top Sites	-	Bookmarks
CoolNovo/ ChromePlus	Top Sites	-	Bookmarks

Analysis – Special Log Files

- Sougou Explorer – History log is uhistory.db that will be deleted by manual or auto-erase

```
Table UserRankUrl (id    char(512) primary key,  
                  title    char(100),  
                  keyfactor int,  
                  hit      int,  
                  deleteflag int,  
                  oftenfactor int,  
                  titleLock int  
                  last      datetime,  
                  reserved  int  
                  );
```

The table is used to record all the web sites which the user visited. It will create the new record if the user visits a new web site and update the last accessed time if the user visits a existed page.

Future Work

- Exact user name, password and other information from Magia Fill
- Correlation analysis between several browsers
- To reconstruct web pages from cache



Questions?

Ask Linda Zhong